LUXOFT GROUP DATA PROTECTION POLICY

CONTENTS

PART ONE: GENERAL

LUXOFT GROUP DATA PROTECTION POLICY

REQUIREMENTS FOR ALL STAFF

1. **PURPOSE**

1.1 This document sets out the policies and procedures that the LUXOFT GROUP has put in place to comply with basic data protection principles. Since a number of entities of the LUXOFT GROUP are situated in Europe, this document especially takes into account European data protection laws and provides a short overview of these laws – especially the European Data Protection Directive (Directive 95/46/EC) respectively the EU General Data Protection Regulation (EU) 2016/679 ("**GDPR**") from 25 May 2018 onward.

2. **SCOPE**

2.1 This policy applies to Luxoft Holding, Inc. and all of its branches and entities worldwide (together "**LUXOFT GROUP**"). All employees and agency personnel (staff) within LUXOFT GROUP must comply with the policy. All LUXOFT GROUP staff will receive information security training (which includes data protection compliance) on a regular basis.

2.2 Some parts of this policy apply to the branches and entities situated in EU or EEA countries respectively Switzerland ("**European Operations**") only.

2.3 This policy is split into two parts: Part One is general and applies to all staff. Part Two contains additional provisions for specific departments and operations in specific countries. More detailed provisions apply to:

- Annex A: Personnel Department;
- Annex B: Sales and Procurement;
- Annex B: Information Technology; and
- Annex D: Facilities.

2.4 Data protection laws vary from country to country. This policy has been reviewed for local compliance in Australia, British Virgin Islands, Bulgaria, Canada, China, Cyprus, Denmark, France, Germany, India, Luxembourg, Malaysia, Mexico, The Netherlands, Poland, Romania, Russia, Singapore, South Africa, Sweden, Switzerland, UK, Ukraine, USA and Vietnam. Where there is a different requirement in these countries, a note is indicated above the text and you must refer to the relevant country-specific Appendix in Part Two.

3. **COMMITMENT TO COMPLY WITH BASIC DATA PROTECTION PRINCIPLES**

3.1 All LUXOFT GROUP staff must comply with their obligations under this policy and applicable local data protection laws whenever they are processing personal data **[South Africa 1] [China 1]**. The Data Protection Safeguards set out in Section 4 below and in Part Two set out what this means.

3.2 **Data protection principles apply when personal data is processed by, or on behalf of, LUXOFT GROUP.**

3.3 'Personal data' has a broad meaning: all information that relates to living, identifiable, individuals (either directly or indirectly). This includes data that would identify a person (name, address, telephone or employee number, etc). It includes opinions about individuals as well as facts. Personal data can include information about employees and business contacts: it is not confined to consumers or to a person's personal (i.e. non-work) life either: job title, office telephone number and professional details (for example) are also personal data. The fact that information is publicly available (e.g. on LinkedIn) does not stop data protection laws applying to it. **[Australia 1] [Bulgaria 1] [China 1] [Denmark 1] [Luxembourg 1] [Malaysia 1] [Singapore 1] [South Africa 2] [Switzerland 1]**.

3.4 'Processing' also has a broad meaning: for example, it covers collection of data, holding and using data and destroying personal data. All LUXOFT GROUP staff will almost certainly process some personal data: about customers or suppliers, or about other employees.

3.5 Basic data protection principles require that LUXOFT GROUP:

- only processes personal data for fair and lawful purposes; **[France 1]**
- in accordance with additional restrictions for sensitive personal data[1]; **[China 2]**
- is transparent with people and tells them how it will use their information;
- meets data quality obligations and holds personal data for a limited retention period;
- as a general rule minimises the amount of personal data it collects **[Denmark 2]** and processes and chooses and structures its processing systems accordingly; **[France 2]**
- as a general rule grants its staff access to personal data on a "need to know" basis only;
- implements appropriate security obligations to protect personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures;
- upholds individuals' rights to access and correct their information and, to prevent certain types of processing; **[Denmark 3] [France 3] [Mexico 1] [Sweden 1]** and
- only transfer personal data to other jurisdictions than their own when protections for personal data are in place as required by local law (e.g. European Operations only transfer personal data out of the European Economic Area (EEA)[2] and Switzerland when protections for personal data are in place such as the standard contractual clauses provided by the EU Commission). **[India 6 and India 7] [China 3] [Malaysia 2] [South Africa 3] [Switzerland 1]**

3.6 Data protection laws often also require that LUXOFT GROUP must notify its processing of personal data to the local data protection authority. The appropriate Data Protection Officer is responsible for ensuring that this is done. **[Australia 2] [China 4] [Denmark 4] [India 2] [France 4] [Luxembourg 2] [Malaysia 3] [South Africa 4] [Ukraine 1]**

3.7 Section 4 sets out the steps LUXOFT GROUP has adopted and that you must follow to ensure that these obligations are met.

4. DATA PROTECTION SAFEGUARDS

4.1 Lawful purposes

4.1.1 LUXOFT GROUP may only process personal data for explicit and legitimate purposes and does not further process data in a manner that is incompatible with those purposes.**[France 1] [Vietnam 1]**

4.1.2 Generally, staff may process personal data (other than sensitive personal data) where (1) this is necessary for LUXOFT GROUP's legitimate interests (as defined by local law), provided this does not cause unreasonable prejudice to the interests of the individuals concerned **[China 5] [Cyprus 1] [Sweden 2]** and (2**Cyprus 1] [Sweden 2],** (2) processing is necessary for the performance of a contract to which the individual is party or in order to take steps at the request of the individual prior to entering into a contract or (3) processing is necessary to comply with a legal obligation. **[Bulgaria 2] [Denmark 5] [Singapore 2] [Vietnam 2]**

4.1.3 In some situations, LUXOFT GROUP may also process personal data when the relevant individual has given consent. This must usually be express and in many countries this is subject to strict formal requirements. Marketing may process personal data on this basis. In other situations, staff should seek guidance from the Data Protection Officer if they wish to collect and use personal data based on individual consent. **[Canada 1] [India 2, India 3, India 4 and India 5] [France 5] [China 6] [Malaysia 3 and Malaysia 4] [Russia 1]**

[1] For a definition of sensitive personal data see 4.2 below.
[2] EU Member States, Norway, Iceland, and Liechtenstein.

4.1.4 Where LUXOFT GROUP holds personal data for certain specific purposes, staff must not then use the data any other way which is incompatible with those purposes: if the relevant individuals would not expect this use of the data, it is likely to be 'incompatible use'. For example, you may not access the customer or staff databases for your own purposes, or for friends or family. This is a serious disciplinary offence and may be a criminal offence for which you can be prosecuted.

4.1.5 Use of data for a new purpose, can also affect LUXOFT GROUP's filings with data protection authorities. Staff must therefore consult the Data Protection Officer, if they wish to use personal data for a new purpose. **[India 2 and India 3] [France 6] [Malaysia 3] [Mexico 2]**

4.2 Sensitive personal data

4.2.1 Sensitive personal data is generally information about an individual's physical or mental health or condition, racial or ethnic origin, political opinions, trade union membership, religious or philosophical beliefs and sexual life, genetic and biometric data (if this data is processed for the purpose of uniquely identifying an individual) although local laws may vary (for example in the UK, the commission or alleged commission of any criminal offence and criminal convictions are also sensitive personal data and in Poland sensitive personal data includes data relating to decisions issued in court or administrative hearings). **[Australia 3] [Bulgaria 3] [Canada 2] [China 2] [Cyprus 2] [Denmark 6] [India 1France 7] [Luxembourg 3] [Malaysia 5] [Netherlands 1] [Russia 2] [Ukraine 2]**

4.2.2 Personnel Department is the only department where staff is allowed to process sensitive personal data. **[France 8] [Ukraine 3]**

4.3 Transparency

4.3.1 LUXOFT GROUP must be transparent about how it uses personal data: if you collect personal data about individuals, you must tell them how this information will be used. This means providing information about **[Australia 4] [France 9] [Malaysia 6]**:

- the LUXOFT GROUP entity collecting the information (including the contact data of the Data Protection Officer, where applicable); **[Bulgaria 4] [Denmark 7] [Poland 1] [Sweden 3] [Ukraine 4]**
- the purposes for which LUXOFT GROUP processes personal data as well as the legal basis for the processing; **[Vietnam 3]**
- where the data processing is based on legitimate interests, the legitimate interests of LUXOFT GROUP on which the data processing is based;
- whether replies to questions are mandatory or voluntary, and the consequences if information is not provided;
- the types of people who will receive the data and the purposes for which they will receive it;
- the rights that individuals have (including to access, correct and sometimes to object to the processing of their data) **[Denmark 3] [Sweden 1]**; and
- any transfers of personal data outside their own jurisdiction, where required by local law; European Operations have to provide information about any transfers of personal data outside EEA. **[Australia 5] [Canada 3] [China 3] [Denmark 8] [India 6 and India 7] [France 10) [Switzerland 1] [Russia 3] [Ukraine 5].**

4.3.2 In addition to the information referred to in Section 4.3.1, the LUXOFT GROUP shall, at the time when personal data are obtained, provide individuals with the following further information necessary to ensure fair and transparent processing in accordance with applicable data protection laws:

- the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

- the existence of the right to request from LUXOFT GROUP access to and rectification or erasure of personal data or restriction of processing concerning individuals or to object to processing as well as the right to data portability;

- if the data processing is based on consent, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

- the right to lodge a complaint with a supervisory authority;

- whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether an individual is obliged to provide the personal data and of the possible consequences of failure to provide such data;

- the existence of automated decision-making, including profiling and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for an individual;

4.3.3 Where personal data have not been directly obtained from an individual, and in accordance with applicable data protection laws, the LUXOFT GROUP shall provide the individual with the following information in addition to the information as set out in 4.3.2:

- the categories of personal data concerned;

- from which source the personal data originate, and if applicable, whether it comes from publicly accessible sources.

4.3.4 In general, the information set out under the foregoing sections must be provided to individuals before LUXOFT GROUP obtains personal data from them. LUXOFT GROUP does not have to provide this information to the extent the individual already has the information. Specific requirements for Personnel Department and Marketing are set out in the relevant Annexes **[France 11]**.

4.3.5 It is not necessary to provide this information for business contact information provided by the individual, where it is evident from the context how you will use the information (e.g. giving a card to allow for follow up). **[Australia 6] [Bulgaria 5] [Canada 4] [China 7] [Denmark 9] [France 12] [Luxembourg 4] [Malaysia 7] [Poland 2] [Switzerland 2]**

4.4 Data quality and retention

4.4.1 You should only use personal data that are adequate, relevant and not excessive. Data may only be collected if there is a business need for the information and if the level of information is proportionate to this.

4.4.2 You should use personal data that are accurate and, where necessary, up to date. You should advise Personnel Department promptly if your details change. If you are told about a change in a customer's or supplier's personnel, you should change any local contact databases that you maintain and ensure central databases are updated accordingly.

4.4.3 LUXOFT GROUP must not retain personal data for longer than is necessary for the purposes for which the data was collected. Guidance on what this means for Personnel Department is set out in Annex A **[China 8]**.

4.5 Security and Confidentiality

4.5.1 LUXOFT GROUP shall implement appropriate administrative, technical, organisational and physical measures to protect personal data, including *inter alia*,

- the pseudonymisation and encryption of personal data;

- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a data breach;
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

4.5.2 This requires appropriate IT and physical security and staff training and care in selection of third parties who process LUXOFT GROUP personal data. These measures may vary from country to country.

4.5.3 LUXOFT GROUP shall, where required and in accordance with applicable laws, carry out data protection impact assessments ("PIA") before introducing new processing operations.

4.5.4 The main processes for securing the LUXOFT GROUP IT environment are set out in the Information Security Manual, Security Incident Management policy and associated documents, which all staff must comply with. Further guidelines are set out in the Corporate Code of Conduct, the Insider Trading Policy, the Rules for Handling of Service Information, the Regulations on the Processing of Personal Data, Rules on Company Information Treatment by Employees, Instructions "Use of Corporate Electronic Mail" and Non-disclosure agreements.

4.5.5 Where staff have permission to work from home or any other off-premises site, special conditions apply to the handling of personal data which must be fully observed.

4.5.6 Any suspected or actual breach, unauthorised disclosure of, damage to or loss of any LUXOFT GROUP personal data (including loss of or damage to equipment containing LUXOFT GROUP personal data) shall be reported immediately to the Chief Information Officer (CIO) or to the IT Department as well as to the appropriate Data Protection Officer. **[China 9] [Denmark 10] [India 2 and India 8] [Malaysia 3] [South Africa 5]**

4.5.7 Be aware that those seeking information sometimes use deception in order to gain access to it. Always verify the identity of the individual and the legitimacy of the request according to LUXOFT GROUP's policies, particularly before releasing information over the phone. If in doubt, please speak to the appropriate Data Protection Officer.

4.6 Restriction on transfers outside the EEA [Australia 7] [China 3] [Denmark 11] [India 6 and India 7] [Malaysia 2] [South Africa 3]

4.6.1 European data protection rules restrict transfers of personal data to including group companies in countries that are outside the European Economic Area (EEA)[3] and Switzerland unless prescribed steps are taken to ensure that the data is protected. Since some of LUXOFT GROUP's IT applications are held and backed outside the EEA and Switzerland, this restriction is particularly relevant for its European Operations. **[Singapore 3] [Switzerland 1]**

4.6.2 LUXOFT GROUP has put in place European Commission approved agreements to regulate the transfers of certain categories of data within the LUXOFT GROUP of companies. **[China 10] [Singapore 4] [Switzerland 1]**

4.6.3 European Operations staff must seek the input of the Data Protection Officer if you want to transfer personal data to a new supplier outside the EEA or Switzerland or if you want to transfer new categories of data to LUXOFT GROUP entities outside the EEA or Switzerland. The input of the Data Protection Officer must include the information whether prior notification or authorisation of the transfer by the competent data protection authority is required. **[Cyprus 3] [Singapore 5]**

4.7 Rights of Individuals

[3] EU Member States, Norway, Iceland, and Liechtenstein.

4.7.1 Each individual shall have the right to obtain from LUXOFT GROUP confirmation as to whether or not personal data concerning the individuals are processed, and, where that is the case, access to the personal data and the following information:

- the purposes of the processing;
- the categories of personal data concerned;
- the recipients or categories of recipients to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
- where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- the existence of the right to request from LUXOFT GROUP rectification or erasure of personal data, restriction of processing personal data concerning the individual, and to object to such processing;
- the right to lodge a complaint with a supervisory authority;
- where personal data are not collected directly from the individual, any available information as to their source;
- the existence of automated decision-making, including profiling.

4.7.2 Where personal data are transferred to a third country or to an international organisation, the individual shall have the right to be informed of the appropriate safeguards relating to the transfer.

4.7.3 LUXOFT GROUP will always honour individuals' rights under and according to data protection laws:

- correct information relating to them;**[Denmark 3] [France 3] [Sweden 1] [Vietnam 4]**
- to erasure ("right to be forgotten");
- to data portability;
- to restriction of processing;
- to prevent direct marketing to them; **[France 13]**
- to prevent certain other types of processing in special situations; and
- to object to the use of entirely automated decisions to take significant decisions about them. **[China 11] [Mexico 3] [Russia 4]**

4.7.4 Staff must take care when entering information in free-text areas as those to whom the text refers (such as customers) may see this information at a later date. Information should only be entered which is appropriate and justifiable and should not include sensitive personal data.

4.7.5 Requests by staff to see their records should be made, in writing, to the Head of Personnel Department. If staff receives any other request to see personal details or a request that LUXOFT GROUP delete data or cease processing data should be forwarded immediately to the Data Protection Officer. There are often strict timescales for complying with such requests, so requests must be forwarded as soon as possible following receipt. **[India 2] [Malaysia 3] [Sweden 4]**

5. EXCEPTIONS:

Any request to deviate from this policy must be approved by the Data Protection Officer. **[India 2] [Malaysia 3]**

6. **VIOLATIONS:**

6.1 Subject to local law requirements, failure to comply with this policy may be a disciplinary offence and will be handled in accordance with LUXOFT GROUP's disciplinary procedures.

6.2 Failure to comply with this policy may also mean that you are directly liable for penalties under local data protection law. In particular, use, for private or illegal purposes, of personal data obtained through your work at LUXOFT GROUP can be a criminal offence. **[France 14] [Ukraine 6]**

7. **ANY QUERIES?**

If you have any queries in relation to this policy or data protection generally, you should contact your appropriate Data Protection Officer. **[India 2] [Malaysia 3]**

8. **APPROVAL AND VARIATION**

This policy has been approved by Board of Directors of Luxoft Holding Inc. The Data Protection Officer is the sponsor for this policy and must approve any changes to it. **[India 2] [Malaysia 3]**

PART TWO: DEPARTMENT OR COUNTRY SPECIFIC GUIDANCE

CONTENTS

[4] No country appendices exist for: BVI and UK.

South Africa

Sweden

Switzerland

Ukraine

USA

Vietnam

ANNEX A: PERSONNEL DEPARTMENT

DATA PROTECTION SAFEGUARDS

LAWFUL PURPOSES

Normal data

Some of LUXOFT GROUP's contracts of employment currently ask for employee consent to data processing. However, in most countries LUXOFT GROUP is entitled to process information about applicants and employees where: it is necessary for its legitimate interests; this is required to meet statutory obligations or to administer the employment contract. **[China 5] [Denmark 12] [France 15] [Germany 1] [Luxembourg 5] [Malaysia 8] [Mexico 4] [Netherlands 2-3] [Poland 3] [Russia 1] [South Africa 6] [Sweden 5] [Ukraine 7] [Vietnam 5]**

Sensitive data

LUXOFT GROUP is entitled to process sensitive personal data about employees where this is necessary to comply with obligations under employment law – such as dealing with statutory sick pay, or making work-place adjustments**. [India 3, India 4 and India[China 2 and China 5] [South Africa 7]**

Keep sickness and accident records separate from absence records, so absence records do not contain sensitive personal data. **[Bulgaria 6] [Cyprus 4] [Poland 4] [Romania 1]**

Criminal offences

Do not ask applicants for details of criminal offences unless this is necessary for the position. Generally, only unspent convictions will need to be requested. **[Cyprus 5] [France 16]**

Seek local advice before asking for criminal offence data outside the UK. **[Australia 8] [Canada 5] [Cyprus 6] [Denmark 13] [Germany 2] [Luxembourg 6] [Poland 5] [Romania 2]] [Russia 2] [Sweden 6] [Switzerland 3] [Ukraine 8] [USA 1]**

New Uses

Use of data for a new purpose, can also affect LUXOFT GROUP's filings with data protection authorities (e.g new Personnel Department database or system). It may also require consultation with workers' representatives. Staff must therefore consult the Data Protection Officer, if they wish to use personal data for a new purpose. **[Bulgaria 7] [India 2France 6 and India 3France 17China 4] [Malaysia 3] [Mexico 5] [Netherlands 2-3][Singapore 6]] [South Africa 8] [Ukraine 9]**

TRANSPARENCY

Applicants

Ensure that all applicants are told how LUXOFT GROUP will use CVs and other personal data. **[Russia 5]**

For unsuccessful applicants, explain if you want to keep CVs on file for future use and do not do this if the applicant objects. **[Cyprus 7] [Denmark 14] [France 18] [Malaysia 9] [Poland 6] [Romania 3] [Russia 6] [Sweden 7] [Switzerland 4] [Ukraine 10]**

For successful applicants, be clear what background checks will be made and from whom the information will be sought (e.g. identification checks, certification of right to work, collection of references). Make it clear if the successful completion of background checks is a pre-condition of employment with LUXOFT GROUP. **[Russia 7]**

Refer to the standard notice for applicants at Supplementary Document 1. **[USA 2]**

Employees

Ensure all staff are told how LUXOFT GROUP uses their personal data: relevant information should be included in the Employee Privacy Notice (see Supplementary Document 2).

Where LUXOFT GROUP provides staff data to third parties to provide benefits, make staff aware of this in the literature used to explain the benefits (e.g. pension, insurance or private health providers). If LUXOFT GROUP collects information to pass on to the third parties for administration purposes, do not use this for general employment purposes. **[Malaysia 10]**

[Vietnam 6]

DATA QUALITY

General

Only collect information about individuals where there is a clear and foreseeable need for the information. Ensure that when you collect information in application forms/new joiner forms that you identify what information is mandatory or what information is voluntary (i.e by way of a footnote). **[France 11]**

Applicants

If you prepare an application form, only request information which is relevant and not excessive. It should also comply with all relevant anti-discrimination laws. **[France 19]**

Remind interviewers that they should only record information during an interview which is relevant to the recruitment decision: applicants may have a right to see interview notes. **[Cyprus 8]**

RETENTION

General

Carry out file reviews and ensure that irrelevant information is removed and securely destroyed.

Follow the retention guidelines at Supplementary Document 3.

SECURITY

You should ensure that:

- only staff needing access to personnel files to carry out their duties are given such access, and audit trails are put in place to show who has accessed and/or amended such files;
- the taking of employee personal data off-site (e.g. in laptop computers) is controlled and that strict security rules are applied;
- if you are sending confidential or sensitive information about an employee by email or fax, consider whether additional security measures such as encryption are required.

TRANSFERS

[Australia 7] [China 3] [Denmark 11] [India 2, India 6 and India 7] [Malaysia 2 and Malaysia 3] [Russia 3 and Russia 8] [South Africa 3]

Seek advice from the Data Protection Officer if:

you wish to use a third party outside your own jurisdiction to process employee personal data; or

if you belong to European Operations and

- wish to use a third party outside the EEA or Switzerland or
- have any queries about what data may be transferred to LUXOFT GROUP entities outside the EEA or Switzerland.

RIGHTS

Access

Forward any requests from candidates or employees to see and/or correct their data or to object to the processing of their data to the Head of Personnel Department. Remind line managers to do this. **[Australia 9] [Denmark 3] [India 2] [Singapore 7] [Sweden 1]**

Seek the advice of the Data Protection Officer, if needed, in handling subject access requests. **[India 2] [Malaysia 3]**

Marketing

Do not allow third parties to send direct marketing material to employees. **[Cyprus 9] [Malaysia 11]**

Automated decisions

Do not deploy automated decision taking techniques – such as automatic scanning of CVs or absence monitoring systems – without first checking with the Data Protection Officer. On some occasions, specific notices and rights of appeal need to be arranged, and in some countries, the works council may need to be consulted. **[India 3]China 11] [Malaysia 3] [Netherlands 2]**

SPECIAL SITUATIONS

Requests to disclose data

References: always check with the employee before providing a reference. **[Vietnam 7]**

If asked to disclose information about an employee to a third party, always verify the identity of the third party to check they are entitled to receive the information. Consider whether there is a legal obligation to disclose the information (e.g. in the UK to the Inland Revenue) or whether information is required for legal proceedings or in connection with the prevention or detection of crime. If these considerations do not apply, consider whether it would be fair to the employee to release the information. Please seek further advice from the Data Protection Officer if you are uncertain about the nature of the request. **[Cyprus 10] [India 2 and India 6] [Malaysia 12 and Malaysia 3] [South Africa 8]**

Where practicable, workers should be told about such disclosures.

Monitoring

The Head of Personnel Department must authorise any requests to monitor specific employees. This would apply to any of monitoring IT Equipment and traffic on the IT Network telephone calls and other forms of monitoring. Before authorising any monitoring, the Head of Personnel Department will: **[Australia 10] [Denmark 15] [France 20] [Malaysia 13] [Switzerland 5] [Vietnam 8]**

- Carry out an impact assessment, to ensure that there is a legitimate purpose for the monitoring, that the impact of the monitoring on the individual is justified and that the intrusiveness of the monitoring is kept to the minimum level necessary to achieve the purpose of the monitoring;

- Consider if employees should be notified that monitoring will be carried out. Where monitoring is used to enforce LUXOFT GROUP rules and policies, the relevant rules and policies and the nature and extent of associated monitoring must be clearly specified. General notice to this effect is included in the Rules on Company information treatment by employees, Information Security Manual and the Employee Privacy Notice; **[China 12] [Cyprus 11] [Luxembourg 6] [USA 2, USA 3]**

- Consider any applicable local law requirements relating to monitoring and interception, particularly as this can constitute a criminal offence in certain countries. In some countries, the works council may also need to be consulted;

- Ensure that the results of employee monitoring will only be available to a limited number of people and may only be used for the purpose for which the monitoring was implemented, unless the results reveal evidence of criminal activity at work, gross misconduct or breaches of health and safety rules which no reasonable employer could ignore; and

- Ensure that emails which are clearly marked as personal will only be read in exceptional circumstances where a problem relating to an employee's excessive or unauthorised use is suspected. You should always contact the appropriate Data Protection Officer and Legal Department before doing so. Note that in some countries, it is prohibited to read any emails marked as private. Please consult the relevant Country Appendices. **Also refer to the local rules for further information. [Australia 10] [Bulgaria 8] [China 12] [Cyprus 12] [Denmark 15] [France 21] [Germany 3] [India 2] [Luxembourg 8] [Mexico 6] [Poland 7]] [Romania 4] [Russia 9] [South Africa 9] [Sweden 8] [Switzerland 6] [USA 4]**

SUPPLEMENTARY DOCUMENT 1: SAMPLE DATA PROTECTION NOTICE FOR APPLICANTS
[Drafted to comply with the UK law only. Amendments might be required to use in other countries]

LUXOFT UK LIMITED is committed to respecting your privacy. We will treat any personal information supplied by you in this application form as confidential and will only process such information as permitted by the Data Protection Act 1998 and as described below.

What information do you have to provide?

If you wish us to consider your application, you have to submit your CV and any other information.

Additional wording where details of criminal convictions are requested:
Where permitted by law, if we ask you to supply information about your criminal record you do not need to supply details of spent convictions[5].

Additional wording required where sensitive personal data is collected:
The Data Protection Act 1998 gives special protection to information about racial/ethnic origin, political opinions, religious beliefs, trade union memberships, health, sexual life and the commission of offences and related proceedings. You should only provide this information if it is required in response to a mandatory question on our website, or if you are otherwise content for us to process this information. We will always hold such information securely. **[China 2]**

How do we use this information?

We will use the information you have provided in order to assess your suitability for LUXOFT UK LIMITED.

Additional wording required where the applicant may be considered for a number of jobs in addition to the advertised job:
If we think that you are suitable for other current vacancies, we may also use the information you have provided for this purpose. We will retain your information for 3 months.

Additional wording where the application form will be kept for possible future use:
If we fill the vacancy for which you have applied, we may keep your application on file for 12 months in case we think you are suitable for other, similar, vacancies in the future. Please let us know if you do not wish us to retain your data for this purpose.

Additional wording where information in the application form will be verified:
We will make the following checks of the information you have provided in the form:

- Checks of experience by contacting previous employers;
- Checks of academic credentials by contacting educational institutions; and
- Checks of the Disclosure and Barring Service.

If we wish to make any other checks (such as to take up references) we will seek your permission first.

Additional wording where vetting will be carried out:
In addition to the checks described above, we will make enquiries of third parties about your background and circumstances. These checks are necessary, as this post involves access to confidential information and/or requires security clearances. In order to carry out these checks we will: [explain nature of checks to be carried out, the nature, extent and range of sources that will be checked, what information will be released to third parties and when the checks will be carried out].

We are an international company. Accordingly, where we think it appropriate, we may transfer the information we receive from you to LUXOFT GROUP's centralized Personnel Department, which is operated by LUXOFT GROUP entities in the world. Some of these entities do not have equivalent data protection legislation to Europe. However, whenever we transfer your data in this way, we will transfer it in accordance with the applicable EU data protection requirements, keep it secure and only use it as outlined in this notice. **[China 5]**

[5] Note if details of criminal convictions are requested and the position being filled is covered by the Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975 then use the following wording: Where we ask you to supply information about your criminal record, you must disclose all convictions including spent convictions.

Who has access to the information?

Your information is held securely and is generally only provided, on a need to know basis, to members of the **Personnel Department** and line managers in the business area to which the job relates for use for the purposes listed above.

Your rights

The Data Protection Act 1998 grants you certain rights – including a right to access, amend or object to the processing of most of the information that we hold about you. If you wish to see this information, please contact the Data Protection Officer, LUXOFT UK LIMITED, 35 New Broad Street, New Broad Street House, London EC2M 1NH, United Kingdom, e-mail: dpo-uk@luxoft.com, Tel: +44 0207 993 0737, Fax: +44 (0) 207 956 2001.

SUPPLEMENTARY DOCUMENT 2: SAMPLE PRIVACY NOTICE FOR EMPLOYEES
[Drafted to comply with the UK law only. Amendments will be required to use in other countries]

LUXOFT UK LIMITED, 35 New Broad Street, New Broad Street House, London EC2M 1NH, United Kingdom ("LUXOFT"), is committed to respecting your privacy. We will only process such information as permitted by the Data Protection Act 1998 and as described below.

What information do we collect about you?

The information we collect about you includes:

- your name, home address, postal address, temporary address, nationality, employee ID number, national insurance number, immigration status, age, data of birth, passport and ID number, photo image,
- beneficiaries' details in relation to life insurance or other benefits, emergency contacts, marital status, information about family members (name, date of birth, gender and national personal ID number) where necessary for the provision of applicable benefits, alimony payments, guarantees or relocation assistance,
- job title, employer, division, position, business unit, location of working place, work email, professional experience, education, performance history, training records,
- health insurance details, salary, remuneration, social and other benefits, bank details
- trip itineraries with dates and times, visa, driving licence details,
- expense records (such as details of out of pocket expenses, corporate credit cards, company cars or private cars where an allowance is claimed and mobile phone costs),
- phone numbers (home and mobile), written and electronic communications, where permissible
- information concerning performance, career plans, conduct and, where permissible, about violation of laws or breach of company policies,
- medical leave information, sickness and accident records, medical certificates, workplace adjustments, other documents required to confer special benefit status, such as information concerning pregnancy status and age of children, etc. where applicable and
- information about trade union affiliation if you have asked us to make payments to trade unions on your behalf.

LUXOFT will keep this information, together with data retained from the application and selection process, for the course of the employment relationship and, to the extent permitted, after termination of employment.

How do we use this information? **[China 5 and China 13]**

LUXOFT processes this personal data for the following purposes:

- As required to establish and perform the employment contract, to maintain or terminate the employment relationship and to enable you to perform your job. This includes recruiting and hiring and administration of payroll and benefits, absence, compensation and sales quota commission, performance and talent management, training and leadership development, transfer management from different subsidiaries and branches, succession management, award recognition, employee surveys, medical insurance, occupational health, retirement plans, stock plans, expense management and professional travel.
- As required by LUXOFT to enable its business, in particular to provide access to LUXOFT' s offices, management of LUXOFT's IT systems and infrastructure, inclusion in company directories and provision of communication services such as e-mail, telephone and internet access.
- Protecting the security of LUXOFT's premises, assets, systems, and intellectual property and enforcing company policies, including monitoring communications where permitted by local law and in accordance with LUXOFT's Regulations on the processing of personal data, Rules on Company information treatment by employees, Information Security Manual, Security Incident Management, Instructions "Use of Corporate Electronic Mail" and for investigations and disciplinary actions.
- Compliance with applicable laws and protection of LUXOFT's legitimate business interests and legal rights, including, but not limited to, use in connection with legal claims, compliance, regulatory, investigative and disciplinary purposes (including disclosure of such information in connection with legal process or litigation) and other ethics and compliance reporting tools.

In addition, with your consent, we collect your picture for use with your contact details in LUXOFT GROUP directories, in internal communications and newsletters and in external news and media in connection with events and updates about LUXOFT. Where permitted by local law and with your consent, we also hold background checks to evaluate eligibility for employment and medical information if a regular or onboarding health check is required or to evaluate eligibility for applicable benefits.

Personal data will be transferred to Luxoft Holding Inc, its affiliates and contractors, in the US and other countries, including outside the EU, and will be stored and processed manually and electronically through global systems and tools for the purposes above. Information contained in internal directories may be accessed on a worldwide basis by

employees of other LUXOFT GROUP entities. Other personal data will primarily be processed by employees of the HR, IT and finance, legal and facilities departments, where relevant and necessary. We have taken steps to ensure that there is adequate protection for your personal data in these circumstances.

Personal data may be shared with government authorities and/or law enforcement officials if required for the purposes above, if mandated by law and if required for the legal protection of LUXOFT's legitimate interests in compliance with applicable laws. Personal data may also be shared with third party service providers, who will process it on behalf of LUXOFT for the purposes above. Such third parties include, but are not limited to, payroll service providers, IT service providers, travel agencies and travel service providers, banks, credit card companies, brokers, medical services and medical insurance providers, training providers, survey service providers, investigators, employee hotline administrators, data custodians, etc. In the event that the business is sold or integrated with another business, your details may be disclosed to our advisers and any prospective purchaser's adviser and will be passed to the new owners of the business.

LUXOFT has taken appropriate technical, administrative, physical and procedural security measures, consistent with local and international information practices, to protect the personal data from misuse, unauthorized access or disclosure, loss, alteration, or destruction. These measures include:

- *Physical safeguards*, such as locked doors and file cabinets, controlled access to our facilities, and secure destruction of media containing personal data.
- *Technology safeguards*, such as use of anti-virus and endpoint protection software, passwords, encryption, and monitoring of our systems and data centres to ensure compliance with our security policies.
- *Organizational safeguards*, through training and awareness programs on security and privacy, to ensure employees understand the importance and means by which they must protect personal data, as well as through privacy policies and policy standards that govern how LUXOFT treats personal data.

Your rights

According to the Data Protection Act 1998, you have the right to access or rectify personal data that relates to you. To rectify or request access to your personal data please contact your HR representative at any time. There are exceptions to these rights so that access may be denied, for example, if making the information available would reveal personal information about another person or if LUXOFT is legally prevented from disclosing such information. You have the right to withdraw your consent at any time with future effect. In that case, however, we may still process your personal data on an alternative legal basis in accordance with applicable data protection laws.

Your obligations

It is important that we maintain up to date records of key information on you. Please notify your manager of any changes in your personal circumstances as soon as they occur (eg change of address, marital status, emergency contacts). From time to time we may ask you to complete a new personal information form to ensure our records are up to date.
Where we require personal data to comply with legal or contractual obligations, then provision of such data is mandatory: if such data is not provided, then we will not be able to manage the employment relationship, or to meet obligations placed on us. In all other cases, provision of requested personal data is optional.

[China 13]
Consent to use of photo

Please confirm by ticking the boxes below if you agree to your photo being used for the following purposes:

[ ] corporate directory;

[ ] internal communications and newsletters;

[ ] external news and media (including online media) in connection with events and updates about LUXOFT GROUP.

_____ _____
Date Name of employee

SUPPLEMENTARY DOCUMENT 3: HR RECORDS RETENTION PERIOD

Unless otherwise specified below or unless there is a reasonable belief that legal proceedings will be started, all documents should be destroyed at the end of the retention period. If it is likely that legal proceedings will start, then records should be retained and passed to the Legal Department. Any queries regarding retention periods should be referred to the Data Protection Officer. See Country Appendices for more detail.

Document	Australia	British Virgin Islands (BVI)	Bulgaria	Canada	Cyprus	China	Denmark	Germany	India	Luxembourg	Malaysia	Mexico	Netherlands
Unsolicited application forms/CVs (not to be pursued)	Unsolicited information may only be retained if it is reasonably necessary for the organisation's functions or activities. Once such information is no longer needed, it should be destroyed or de-identified.	No statutory retention period so UK position likely to be acceptable.	The law does not determine specific retention period. For a period that does not exceed the time necessary for the purposes for which such data are being processed; personal data which are to be retained for a longer period of time for statistical purposes shall be stored in a format precluding the identification of individuals. For applicants who are approved on the basis of such CVs, the data may become part of the employee's personal file and to be kept during the employment period. After the termination of the employment contract the CVs should be destroyed within reasonable time, unless their storage is still necessary for the purposes for which the CVs have been collected/ stored. The employees may grant their consent for a specific term for which their CVs could be kept after the termination of the employment contract depending on the purposes for the CVs may be	No statutory retention period so UK position likely to be acceptable.	Consent of applicant is required to use application forms / CVS for future use if applicant is unsuccessful. If consent is not obtained application forms / CVs may be used only until employee selection period ends. If a candidate expressly requests deletion of their data, this should be done immediately. No statutory retention period.	Permanently	No statutory retention period. The Danish Data Protection Agency prescribes that applicant data should be deleted as soon as possible after the applicant has been informed that he/she has been rejected. Generally the data should be kept for **no longer than six (6) months.** Consent of applicant is required to use application forms/CVs for future use if applicant is rejected. If consent is not obtained, application forms/CVs may be used only until employee selection period ends. If a candidate expressly requests deletion of its data, this should be done immediately.	Applicant data should generally be kept for **no longer than two (2) months** after an applicant has been informed that they have been rejected. If a candidate expressly requests deletion of their data, this should be done immediately. If the data shall be kept for the above retention period, in this case the data has to be blocked (*Sperrung,* Section 35 para 3 German Data Protection Act) in order to respect the deletion request.	No statutory retention period. However, in the event the document contains sensitive personal data or information pertaining to the candidate(s), the law mandates that a body corporate or a person on its behalf shall not retain such information for longer than it is required for the purposes for which the information may be lawfully used (the information collected shall be used for the purpose for which it has been collected) or the same is otherwise required under any law for the time being in force.	No statutory retention period. The default position applies: such data should not be retained for longer than is necessary for the purposes for which the data was collected. Please note that the French data protection authority (CNIL) considers that the retention of such data should not exceed **two (2) years** as from the last contact with the applicant. In practice, the Luxembourg data protection authority frequently adheres to the recommendations made by the CNIL. It is therefore recommended to destroy such data after **two (2) years**.	No statutory retention period. The general rule is that such data should not be retained for longer than is necessary for the fulfilment of the purpose for which the data was collected. The Malaysian data protection authority has issued a guideline that personal data collection forms used in commercial transactions must be disposed within a period not exceeding fourteen (14) days except if/ unless the forms carry legal values in relation to the commercial transaction. It is also recommended that consent of the applicant is required to use application forms/ CVs for future use. This applies to unsuccessful applicants and unsolicited applications not to be pursued. If the applicant expressly requests	According to Articles 516 and 804 of the Federal Labour Law ("FLL") it is not necessary to hold files for more than a year. Thus, our recommendation is to keep them in archives for **one (1) year**.	No statutory retention period. The general rule applies: such data should be deleted as long as it is no longer necessary. The longer such data is kept, the harder it will be to justify such retention as the rights of the individual will prevail. Best practice based on an Exemption Decree is four (4) weeks after the end of the application, or one (1) year with consent of the applicant.

Document	Australia	British Virgin Islands (BVI)	Bulgaria	Canada	Cyprus	China	Denmark	Germany	India	Luxembourg	Malaysia	Mexico	Netherlands
			processed.								deletion of its personal data, this should be done immediately.		
Application Forms/CVs	Once such information is no longer needed, it should be destroyed or de-identified. For employees, it would form part of an employee record, which for the purposes of the *Fair Work Act 2009* must be retained for 7 years after the termination of employment.	No statutory retention period so UK position likely to be acceptable.	The law does not determine a specific retention period. The CVs could be kept in a form which permits identification of the applicants for no longer than it is necessary for the purposes for which the CVs were collected or for which they are further processed. For unsuccessful candidates the CVs could be processed till the end of the respective recruitment process. For being keep and to use for further recruitment procedures, the consent of the candidates is needed or at least they should be aware that their CVs will be used in such a way and should be able to object at any time. For successful candidates the data could become part of the employee's personal file and to be kept during the employment period. After the termination of the employment contract the CVs should be destroyed within reasonable time, unless their storage is still necessary for the purposes for which the CVs have been collected/	No statutory retention period so UK position likely to be acceptable.	Consent of applicant is required to use application forms / CVS for future use if applicant is unsuccessful. If consent is not obtained application forms / CVs may be used only until employee selection period ends. If a candidate expressly requests deletion of their data, this should be done immediately. No statutory retention period.	Permanently	No statutory retention period. Consent of applicant is required to use application forms/CVs for future use if applicant is rejected. If consent is not obtained, application forms/CVs may be used only until employee selection period ends or until **five (5) years** after the termination of employment.	Applicant data should generally be kept for **no longer than two (2) months** after an applicant has been informed that they have been rejected. If a candidate expressly requests deletion of their data, this should be done immediately. If the data shall be kept for the above retention period, the data has to be blocked (cf. above).	No statutory retention period. However, in the event the document contains sensitive personal data or information pertaining to the candidate(s), the law mandates that a body corporate or a person on its behalf shall not retain such information for longer than it is required for the purposes for which the information may be lawfully used (the information collected shall be used for the purpose for which it has been collected) or the same is otherwise required under any law for the time being in force.	No statutory retention period. The default position applies: such data should not be retained for longer than is necessary for the purposes for which the data was collected. Please note that the French data protection authority (CNIL) has issued a recommendation not to retain such data for longer than the duration of employment. In practice, the Luxembourg data protection authority frequently adheres to the recommendations made by the CNIL. It is therefore recommended to destroy such data after termination of the employment contract.	No statutory retention period. The general rule is that such data should not be retained for longer than is necessary for the fulfilment of the purpose for which the data was collected. The Malaysian data protection authority has issued a guideline stating that personal data collection forms used in commercial transactions must be disposed within a period not exceeding fourteen (14) days except if/ unless the forms carry legal values in relation to the commercial transaction. For successful applicants, the application forms/ CVs could become part of the employee's personal file to be kept during the employment period if consent is obtained.	Although according to Articles 516 and 804 of the FLL it is not necessary to hold files for more than a year, our recommendation is to keep them in archives for **five (5) years**.	No statutory retention period. The general rule applies: such data should be deleted as long as it is no longer necessary. The longer such data is kept, the harder it will be to justify such retention as the rights of the individual will prevail. Best practice based on an Exemption Decree is four (4) weeks after the end of the application, or one (1) year with consent of the applicant. If the applicant becomes an employee, such data may become part of the employment record, if necessary (i.e. the employer has a good reason to keep such records). Employee records must be kept for **seven (7) years** after the termination of employment.

Document	Australia	British Virgin Islands (BVI)	Bulgaria	Canada	Cyprus	China	Denmark	Germany	India	Luxembourg	Malaysia	Mexico	Netherlands
			stored. The employees may consent their CVs to be kept for a specific term after the termination of the employment contract depending on the purposes for which the CVs may be processed. (Recommended term in such case – up to **five (5) years** after the termination of the employment contract (this is the longest period of prescription))										
Interview notes	Once such information is no longer needed, it should be destroyed or de-identified. For employees, it would form part of an employee record, which for the purposes of the *Fair Work Act 2009* must be retained for **seven (7) years** after the termination of employment.	No statutory retention period so UK position likely to be acceptable.	No statutory retention period so UK position likely to be acceptable.	No statutory retention period so UK position likely to be acceptable.	No statutory retention period. If a candidate expressly requests deletion of their data, this should be done immediately. Candidate has a right of access to interview notes.	Permanently	No statutory retention period. The Danish Data Protection Agency prescribes that applicant data/interview notes should be deleted as soon as possible after the applicant has been informed that he/she has been rejected. Generally the data should be kept for **no longer than six (6) months.** Consent of applicant is required to use application data/interview notes for future use if applicant is rejected. If consent is not obtained, application data/interview	Applicant data should generally be kept for **no longer than two (2) months** after an applicant has been informed that they have been rejected. If a candidate expressly requests deletion of their data, this should be done immediately. If the data shall be kept for the above retention period, the data has to be blocked (cf. above).	No statutory retention period. However, in the event the document contains sensitive personal data or information pertaining to the candidate(s), the law mandates that a body corporate or a person on its behalf shall not retain such information for longer than it is required for the purposes for which the information may be lawfully used (the information collected shall be used for the purpose for which it has been collected) or the same is otherwise required under any law for the time being in force.	For rejected applicants / unsolicited applications not pursued, please refer to the retention period in the first row of this table. For successful applicants, please refer to the retention period in the second row of this table.	No statutory retention period. The general rule is that such data should not be retained for longer than is necessary for the fulfilment of the purpose for which the data was collected. For unsuccessful applicants and unsolicited applications not to be pursued, kindly refer to the first row of this table. For successful applicants, kindly refer to the second row of this table.	Although according to Articles 516 and 804 of the FLL it is not necessary to hold files for more than a year, our recommendation is to keep them in archives for **five (5) years**.	No statutory retention period. The general rule applies: such data should be deleted as long as it is no longer necessary. The longer such data is kept, the harder it will be to justify such retention as the rights of the individual will prevail. Best practice based on an Exemption Decree is four (4) weeks after the end of the application, or one (1) year with consent of the applicant. If the applicant becomes an employee, such data may become part of the employment record, if necessary (i.e. the employer has a good reason to keep such records).

Document	Australia	British Virgin Islands (BVI)	Bulgaria	Canada	Cyprus	China	Denmark	Germany	India	Luxembourg	Malaysia	Mexico	Netherlands
							notes may be used only until employee selection period ends or until **five (5) years** after the termination of employment.						Employee records must be kept for **seven (7) years** after the termination of employment.
References given to a potential future employer	Information should be destroyed or de-identified after it is no longer required.	No statutory retention period so UK position likely to be acceptable.	No statutory retention period so UK position likely to be acceptable.	No statutory retention period so UK position likely to be acceptable.	No statutory retention period so UK position likely to be acceptable.	Permanently	No statutory retention period. Such data should not be retained for longer than is necessary for the purposes for which the data was collected.	No statutory retention period so UK position likely to be acceptable.	No statutory retention period. However, in the event the document contains sensitive personal data or information pertaining to the candidate(s), the law mandates that a body corporate or a person on its behalf shall not retain such information for longer than it is required for the purposes for which the information may be lawfully used (the information collected shall be used for the purpose for which it has been collected) or the same is otherwise required under any law for the time being in force.	No statutory retention period. The default position applies: such data should not be retained for longer than is necessary for the purposes for which the data was collected. Please note that the French data protection authority (CNIL) has issued a recommendation not to retain such data for longer than the duration of employment. In practice, the Luxembourg data protection authority frequently adheres to the recommendations made by the CNIL. It is therefore recommended to destroy such data after termination of the employment contract.	No statutory retention period. The general rule is that such data should not be retained for longer than is necessary for the fulfilment of the purpose for which the data was collected.	Although according to Articles 516 and 804 of the FLL it is not necessary to hold files for more than a year, our recommendation is to keep them in archives for **five (5) years**.	No statutory retention period so UK position likely to be acceptable.
Absence records showing incidence of sickness absence, annual leave and other approved and unapproved absence	Employee records must be kept for **seven (7) years** after the termination of employment.	Employee records should be kept at an address in the BVI for **not less than six (6) years** from the termination of employment.	**Fifty (50) years** when information is transferred to the employees' pay-roll sheets or becomes part of orders for non-paid leave for more than thirty (30) days. After expiry of the 50-year term, do not destroy these documents and/or	**Three (3) years** from termination of employment.	No statutory retention period so UK position likely to be acceptable.	Permanently	No statutory retention period. Such data should not be retained for longer than is necessary for the purposes for which the data was	No statutory retention period so UK position likely to be acceptable.	No statutory retention period. However, in the event the document contains sensitive personal data or information pertaining to the candidate(s), the law mandates that a body corporate or a person on its	No statutory retention period. The default position applies: such data should not be retained for longer than is necessary for the purposes for which the data was collected.	No statutory retention period. The general rule is that such data should not be retained for longer than is necessary for the fulfilment of the purpose for which the data	According to Article 804 of the FLL, attendance records should be kept in files during the last year of the employment relationship and one year after termination. Thus, our suggestion is to	Employee records must be kept for **seven (7) years** after the termination of employment. They may be kept longer if necessary in the interest of the company. Examples are records on

Document	Australia	British Virgin Islands (BVI)	Bulgaria	Canada	Cyprus	China	Denmark	Germany	India	Luxembourg	Malaysia	Mexico	Netherlands
			data before prior confirmation from the Legal Department.				collected. The Danish Data Protection Agency prescribes that employee records may be kept until **five (5) years** after the termination of employment.		behalf shall not retain such information for longer than it is required for the purposes for which the information may be lawfully used (the information collected shall be used for the purpose for which it has been collected) or the same is otherwise required under any law for the time being in force.	Please note that the French data protection authority (CNIL) has issued a recommendation not to retain such data for longer than the duration of employment. In practice, the Luxembourg data protection authority frequently adheres to the recommendations made by the CNIL. It is therefore recommended to destroy such data after termination of the employment contract.	was collected. Malaysian law requires employers to keep information registers of their employees for not less than six (6) years. Such information includes details of holidays, annual and sick leave with pay granted during each wage period.	hold them in files for **five (5) years**.	medical/physical incidents which may only become apparent after 30 years. The prolonged retention needs to be duly substantiated and documented, also in light of the rights to privacy such individual has. Please note that there is a legal tension between the Dutch data protection rules (delete as soon as possible) and the need for such data for evidence in employment proceedings.
Appraisals and performance reviews	Employee records must be kept for **seven (7) years** after the termination of employment.	No statutory retention period so UK position likely to be acceptable.	The law does not determine a specific retention period. These data should be kept in a form which permits identification of the employees for no longer than it is necessary for the purposes for which they were collected or for which they are further processed. Such data are part of the employee's personal file and could be kept during the employment period. After the termination of the employment contract these data should be destroyed within reasonable time, unless their storage is still necessary for the purposes for which they have been collected/	**Three (3) years** from termination of employment.	No statutory retention period so UK position likely to be acceptable.	Permanently	No statutory retention period. Such data should not be retained for longer than is necessary for the purposes for which the data was collected. The Danish Data Protection Agency prescribes that employee records may be kept until **five (5) years** after the termination of employment.	No statutory retention period so UK position likely to be acceptable.	No statutory retention period. However, in the event the document contains sensitive personal data or information pertaining to the candidate(s), the law mandates that a body corporate or a person on its behalf shall not retain such information for longer than it is required for the purposes for which the information may be lawfully used (the information collected shall be used for the purpose for which it has been collected) or the same is otherwise required under any law for the time being in force.	No statutory retention period. The default position applies: such data should not be retained for longer than is necessary for the purposes for which the data was collected. Please note that the French data protection authority (CNIL) has issued a recommendation not to retain such data for longer than the duration of employment. In practice, the Luxembourg data protection authority frequently adheres to the recommendations made by the CNIL. It is therefore recommended to destroy such data after termination of the employment contract.	No statutory retention period. The general rule is that such data should not be retained for longer than is necessary for the fulfilment of the purpose for which the data was collected.	Although according to Articles 516 and 804 of the FLL it is not necessary to hold files for more than a year, our recommendation is to keep them in archives for **five (5) years**.	Employee records must be kept for **seven (7) years** after the termination of employment. They may be kept longer if necessary in the interest of the company. The prolonged retention needs to be duly substantiated and documented, also in light of the rights to privacy such individual has. Please note that there is a legal tension between the Dutch data protection rules (delete as soon as possible) and the need for such data for evidence in employment proceedings.

Document	Australia	British Virgin Islands (BVI)	Bulgaria	Canada	Cyprus	China	Denmark	Germany	India	Luxembourg	Malaysia	Mexico	Netherlands
			stored. The employees may consent to a specific term for which these data to be kept after the termination of the employment contract depending on the purposes for which they may be processed. (Recommended term in such case – up to **five (5) years** after the termination of the employment contract (this is the longest period of prescription)).										
Records relating to promotion	Employee records must be kept for **seven (7) years** after the termination of employment.	No statutory retention period so UK position likely to be acceptable.	**Fifty (50) years** from termination of employment, when information was transferred to the employees' pay-roll sheets, employment contract, orders for reappointment and other similar. <u>After expiry of the 50-year term, do not destroy these documents and/or data before prior confirmation from the Legal Department.</u> For other details related to the promotion the law does not determine specific retention period. These data should be kept in a form which permits identification of the data subjects for no longer than it is necessary for the purposes for which they were collected or for which they are further processed. Such data could be	**Three (3) years** from termination of employment.	No statutory retention period so UK position likely to be acceptable.	Permanently	No statutory retention period. Such data should not be retained for longer than is necessary for the purposes for which the data was collected. The Danish Data Protection Agency prescribes that employee records may be kept until **five (5) years** after the termination of employment.	No statutory retention period so UK position likely to be acceptable.	No statutory retention period. However, in the event the document contains sensitive personal data or information pertaining to the candidate(s), the law mandates that a body corporate or a person on its behalf shall not retain such information for longer than it is required for the purposes for which the information may be lawfully used (the information collected shall be used for the purpose for which it has been collected) or the same is otherwise required under any law for the time being in force.	No statutory retention period. The default position applies: such data should not be retained for longer than is necessary for the purposes for which the data was collected. Please note that the French data protection authority (CNIL) has issued a recommendation not to retain such data for longer than the duration of employment. In practice, the Luxembourg data protection authority frequently adheres to the recommendations made by the CNIL. It is therefore recommended to destroy such data after termination of the employment contract.	No statutory retention period. The general rule is that such data should not be retained for longer than is necessary for the fulfilment of the purpose for which the data was collected. Malaysian law requires employers to keep information registers of their employees for not less than six (6) years. Such information includes those concerning occupation or appointment.	Although according to Articles 516 and 804 of the FLL it is not necessary to hold files for more than a year, our recommendation is to keep them in archives for **five (5) years**.	Employee records must be kept for **seven (7) years** after the termination of employment. They may be kept longer if necessary in the interest of the company. The prolonged retention needs to be duly substantiated and documented, also in light of the rights to privacy such individual has. Please note that there is a legal tension between the Dutch data protection rules (delete as soon as possible) and the need for such data for evidence in employment proceedings.

Document	Australia	British Virgin Islands (BVI)	Bulgaria	Canada	Cyprus	China	Denmark	Germany	India	Luxembourg	Malaysia	Mexico	Netherlands
			part of the employee's personal file and could be kept during the employment period. After the termination of the employment contract these data should be destroyed within reasonable time, unless their storage is still necessary for the purposes for which they have been collected/ stored. Since there is no statutory retention period UK position likely to be acceptable. The employees may consent to a specific term for which these data to be kept after the termination of the employment contract depending on the purposes for which they may be processed. (Recommended term in such case – up to **five (5) years** after the termination of the employment contract (this is the longest period of prescription)).										
Reference provided by a former employer	If it becomes part of an employee record, it should be kept for **seven (7) years** after the termination of employment.	No statutory retention period so UK position likely to be acceptable.	The law does not determine specific retention period. These data could be kept in a form which permits identification of the data subjects for no longer than it is necessary for the purposes for which they were collected or for which they are further processed. Such data could be	No statutory retention period so UK position likely to be acceptable.	No statutory retention period so UK position likely to be acceptable.	Permanently	No statutory retention period. Such data should not be retained for longer than is necessary for the purposes for which the data was collected. The Danish Data Protection	No statutory retention period so UK position likely to be acceptable.	No statutory retention period. However, in the event the document contains sensitive personal data or information pertaining to the candidate(s), the law mandates that a body corporate or a person on its behalf shall not retain such information for	For rejected applicants / unsolicited applications not pursued, please refer to the retention period in the first row of this table. For successful applicants, please refer to the retention period in the second row of this table.	No statutory retention period. The general rule is that such data should not be retained for longer than is necessary for the fulfilment of the purpose for which the data was collected. For	Although according to Articles 516 and 804 of the FLL it is not necessary to hold files for more than a year, our recommendation is to keep them in archives for **five (5) years**.	No statutory retention period. The general rule applies: such data should be deleted as long as it is no longer necessary. The longer such data is kept, the harder it will be to justify such retention as the rights of the individual will prevail.

Document	Australia	British Virgin Islands (BVI)	Bulgaria	Canada	Cyprus	China	Denmark	Germany	India	Luxembourg	Malaysia	Mexico	Netherlands
			are part of the employee's personal file and could be kept during the employment period. After the termination of the employment contract these data should be destroyed within reasonable time, unless their storage is still necessary for the purposes for which they have been collected/ stored. The employees may consent these data to be kept for a specific term after the termination of the employment contract depending on the purposes for which they may be processed. (Recommended term in such case – up to 5 years after the termination of the employment contract (this is the longest period of prescription)).				Agency prescribes that employee records may be kept until **five (5) years** after the termination of employment.		longer than it is required for the purposes for which the information may be lawfully used (the information collected shall be used for the purpose for which it has been collected) or the same is otherwise required under any law for the time being in force.		unsuccessful applicants and unsolicited applications not to be pursued, kindly refer to the first row of this table. For successful applicants, kindly refer to the second row of this table.		Best practice based on an Exemption Decree is four (4) weeks after the end of the application, or one (1) year with consent of the applicant. If the applicant becomes an employee, such data may become part of the employment record, if necessary (i.e. the employer has a good reason to keep such records). Employee records must be kept for **seven (7) years** after the termination of employment.
Summary of record of service (including name, position held and dates of employment)	Employee records should be kept for **seven (7) years** after the termination of employment.	Employee records should be kept at an address in the BVI for **not less than six (6) years** from the termination of employment.	**Fifty (50) years** from termination of employment.	**Three (3) years** from termination of employment.	No statutory retention period so UK position likely to be acceptable.	Permanently	No statutory retention period. Such data should not be retained for longer than is necessary for the purposes for which the data was collected. The Danish Data Protection Agency prescribes that employee records may be kept until **five (5) years**	No statutory retention period with exemption of (i) consent to overtime work according to working time law (ii) maternity protection law; respectively **two (2) years** retention. For the rest UK position likely to be acceptable.	No statutory retention period. However, in the event the document contains sensitive personal data or information pertaining to the candidate(s), the law mandates that a body corporate or a person on its behalf shall not retain such information for longer than it is required for the purposes for which the information may be lawfully used	No statutory retention period. The default position applies: such data should not be retained for longer than is necessary for the purposes for which the data was collected. Please note that the French data protection authority (CNIL) has issued a recommendation not to retain such data for longer than the duration of employment. In practice, the	No statutory retention period. The general rule is that such data should not be retained for longer than is necessary for the fulfilment of the purpose for which the data was collected. Malaysian law requires employers to keep information registers of their	Although according to Articles 516 and 804 of the FLL it is not necessary to hold files for more than a year, our recommendation is to keep them in archives for **five (5) years**.	Employee records must be kept for **seven (7) years** after the termination of employment. They may be kept longer if necessary in the interest of the company. The prolonged retention needs to be duly substantiated and documented, also in light of the rights to privacy such individual has. Please note that

Document	Australia	British Virgin Islands (BVI)	Bulgaria	Canada	Cyprus	China	Denmark	Germany	India	Luxembourg	Malaysia	Mexico	Netherlands
							after the termination of employment.		(the information collected shall be used for the purpose for which it has been collected) or the same is otherwise required under any law for the time being in force.	Luxembourg data protection authority frequently adheres to the recommendations made by the CNIL. It is therefore recommended to destroy such data after termination of the employment contract.	employees for not less than six (6) years. Such information includes name, occupation or appointment and date of commencing and leaving employment.		there is a legal tension between the Dutch data protection rules (delete as soon as possible) and the need for such data for evidence in employment proceedings.
Payroll and tax records	Employee records should be kept for **seven (7) years** after the termination of employment.	Records and underlying documentation are to be retained for a minimum of **five (5) years**.	**Payroll - fifty (50) years** from making the files After expiry of the 50-year term, do not destroy these documents and/or data before prior confirmation from the Legal Department. **Tax records – ten (10) years** from the end of the tax year in which the tax obligation arose.	**Seven (7) years**.	**Six (6) years** after the end of the year to which they refer.	Permanently	No statutory retention period. Such data should not be retained for longer than is necessary for the purposes for which the data was collected. The Danish Data Protection Agency prescribes that employee records may be kept until **five (5) years** after the termination of employment. Such data can be kept longer if needed in order to e.g. comply with legal obligations or to defend or pursue a legal claim.	**Six (6) to ten (10) years** depending on the type of record.	**Payroll Information**: shall be maintained for a period of **three (3) years** after the date of the last entry made therein. **Taxation Records**: assessees are required to preserve the books of account for a period of **seven (7) years** from the end of the relevant financial year to which such records pertain to.	**Ten (10) years** (minimum) from the date of creation of the document concerned.	No statutory retention period. The general rule is that such data should not be retained for longer than is necessary for the fulfilment of the purpose for which the data was collected. Malaysian law requires employers to keep information registers of their employees for not less than six (6) years. Such information includes wage rates.	According to Article 804 of the FLL, evidence of payment of profit sharing, vacation, Christmas bonus, premiums, as well as any social security payments, contributions and quotas should be kept in files during **the last year of the employment relationship** and **one (1) year** after termination. Thus, our suggestion is to hold them in files for **five (5) years**. Regarding **tax records**, our recommendation is to keep them for **ten (10) years.**	Employee records must be kept for **seven (7) years** after the termination of employment. They may be kept longer if necessary in the interest of the company. The prolonged retention needs to be duly substantiated and documented, also in light of the rights to privacy such individual has. Please note that there is a legal tension between the Dutch data protection rules (delete as soon as possible) and the need for such data for evidence in employment proceedings.
Records relating to accident or injury at work	Where the accident or injury is a notifiable incident, records must be kept for at least **five (5)**	No statutory retention period so UK position likely to be acceptable.	**Fifty (50) years** from termination of employment. After expiry of the 50-year term, do not destroy these documents and/or data before prior	**Three (3) years** from termination of employment.	No statutory retention period so UK position likely to be acceptable. **[Cyprus 4]**	Permanently	No statutory retention period. Such data should not be retained for longer than is necessary for	No statutory retention period so UK position likely to be acceptable. Note: There are health and safety law retention periods which	No statutory retention period. However, in the event the document contains sensitive personal data or information	No statutory retention period. However, in accordance with the legal limitation period, it is recommended to keep such data for	No statutory retention period. The general rule is that such data should not be retained for	Although Article 297 of the Social Security Law (SSL) establishes a statute of limitations of 5 years, , our recommendation is to keep them in archives for **ten**	Employee records must be kept for **seven (7) years** after the termination of employment. They may be kept longer if

Document	Australia	British Virgin Islands (BVI)	Bulgaria	Canada	Cyprus	China	Denmark	Germany	India	Luxembourg	Malaysia	Mexico	Netherlands
	years.		confirmation from the Legal Department.				the purposes for which the data was collected. The Danish Data Protection Agency prescribes that employee records may be kept until **five (5) years** after the termination of employment. Such data can be kept longer if needed in order to e.g. comply with legal obligations or to defend or pursue a legal claim.	mainly relate to operations and are not considered herein.	pertaining to the candidate(s), the law mandates that a body corporate or a person on its behalf shall not retain such information for longer than it is required for the purposes for which the information may be lawfully used (the information collected shall be used for the purpose for which it has been collected) or the same is otherwise required under any law for the time being in force.	at least **ten (10) years** from termination of employment.	longer than is necessary for the fulfilment of the purpose for which the data was collected. Malaysian law requires employers to keep information registers of all records of contributions payment made to the Social Security Organization for seven (7) years.	**(10) years**.	necessary in the interest of the company. Examples are records on medical/physical incidents which may only become apparent after 30 years. The prolonged retention needs to be duly substantiated and documented, also in light of the rights to privacy such individual has. Please note that there is a legal tension between the Dutch data protection rules (delete as soon as possible) and the need for such data for evidence in employment proceedings.
"Spent" disciplinary proceedings Warnings	Employee records should be kept for **seven (7) years** after the termination of employment.	No statutory retention period so UK position likely to be acceptable.	**After one (1) year** of impeccable work. Disciplinary sanctions other than dismissal may be stricken by the employer before the lapse of the time limit of 1 year, if the employee has not committed other breaches of work discipline.	No statutory retention period so UK position likely to be acceptable.	No statutory retention period so UK position likely to be acceptable.	Permanently; warnings may be kept for 30 years only	No statutory retention period. Such data should not be retained for longer than is necessary for the purposes for which the data was collected. The Danish Data Protection Agency prescribes that employee records may be kept until **five (5) years** after the termination of employment. Such data can be kept longer if needed in	No statutory retention period so UK position likely to be acceptable.	No statutory retention period. However, in the event the document contains sensitive personal data or information pertaining to the candidate(s), the law mandates that a body corporate or a person on its behalf shall not retain such information for longer than it is required for the purposes for which the information may be lawfully used (the information collected shall be used for the purpose for which it has been collected) or the	No statutory retention period. The default position applies: such data should not be retained for longer than is necessary for the purposes for which the data was collected. Please note that the French data protection authority (CNIL) has issued a recommendation not to retain such data for longer than the duration of employment. In practice, the Luxembourg data protection authority frequently adheres to the recommendations made by the CNIL.	No statutory retention period. The general rule is that such data should not be retained for longer than is necessary for the fulfilment of the purpose for which the data was collected.	Although according to Articles 516 and 804 of the FLL it is not necessary to hold files for more than a year, our recommendation is to keep them in archives for **five (5) years**.	Employee records must be kept for **seven (7) years** after the termination of employment. They may be kept longer if necessary in the interest of the company. This however needs to be duly substantiated and documented, also in light of the rights to privacy such individual has. Please note that there is a legal tension between the Dutch data protection rules (delete as soon as possible) and the need for such

Document	Australia	British Virgin Islands (BVI)	Bulgaria	Canada	Cyprus	China	Denmark	Germany	India	Luxembourg	Malaysia	Mexico	Netherlands
							order to e.g. comply with legal obligations or to defend or pursue a legal claim.		same is otherwise required under any law for the time being in force.	It is therefore recommended to destroy such data after termination of the employment contract.			data for evidence in employment proceedings.
Grievances	Employee records should be kept for **seven (7) years** after the termination of employment.	No statutory retention period so UK position likely to be acceptable.	No statutory retention period, so same as UK.	No statutory retention period so UK position likely to be acceptable.	No statutory retention period so UK position likely to be acceptable.	Permanently	No statutory retention period. Such data should not be retained for longer than is necessary for the purposes for which the data was collected. The Danish Data Protection Agency prescribes that employee records may be kept until **five (5) years** after the termination of employment. Such data can be kept longer if needed in order to e.g. comply with legal obligations or to defend or pursue a legal claim.	No statutory retention period so UK position likely to be acceptable.	No statutory retention period. However, in the event the document contains sensitive personal data or information pertaining to the candidate(s), the law mandates that a body corporate or a person on its behalf shall not retain such information for longer than it is required for the purposes for which the information may be lawfully used (the information collected shall be used for the purpose for which it has been collected) or the same is otherwise required under any law for the time being in force.	No statutory retention period. The default position applies: such data should not be retained for longer than is necessary for the purposes for which the data was collected. Please note that the French data protection authority (CNIL) has issued a recommendation not to retain such data for longer than the duration of employment. In practice, the Luxembourg data protection authority frequently adheres to the recommendations made by the CNIL. It is therefore recommended to destroy such data after termination of the employment contract.	No statutory retention period. The general rule is that such data should not be retained for longer than is necessary for the fulfilment of the purpose for which the data was collected.	Although according to Articles 516 and 804 of the FLL it is not necessary to hold files for more than a year, our recommendation is to keep them in archives for **five (5) years**.	Employee records must be kept for **seven (7) years** after the termination of employment. They may be kept longer if necessary in the interest of the company. This however needs to be duly substantiated and documented, also in light of the rights to privacy such individual has. Please note that there is a legal tension between the Dutch data protection rules (delete as soon as possible) and the need for such data for evidence in employment proceedings.
Criminal Convictions	If provided by an employee and form part of an employee record, then **seven (7) years** after the termination of employment.	No statutory retention period so UK position likely to be acceptable.	If a candidate provides information that he has a criminal record, this record should be deleted once the information has been verified unless the information is clearly relevant to the ongoing employment	No statutory retention period so UK position likely to be acceptable.	No statutory retention period so UK position likely to be acceptable.	Permanently	No statutory retention period. Such data should not be retained for longer than is necessary for the purposes for which the data was	Same as UK.	No statutory retention period. However, in the event the document contains sensitive personal data or information pertaining to the candidate(s), the law mandates that a body corporate	Data related to criminal convictions may not be kept for longer than **two (2) years**.	No statutory retention period. The general rule is that such data should not be retained for longer than is necessary for the fulfilment of the purpose for	Although Articles 516 and 804 of the FLL establish that it is not necessary to hold files for more than a year, considering the statute of limitations provided by Article 104 of the Federal Criminal Code (FCC), our	Employee records must be kept for **seven (7) years** after the termination of employment. They may be kept longer if necessary in the interest of the company. This however needs to

Document	Australia	British Virgin Islands (BVI)	Bulgaria	Canada	Cyprus	China	Denmark	Germany	India	Luxembourg	Malaysia	Mexico	Netherlands
			relationship.				collected.		or a person on its behalf shall not retain such information for longer than it is required for the purposes for which the information may be lawfully used (the information collected shall be used for the purpose for which it has been collected) or the same is otherwise required under any law for the time being in force.		which the data was collected.	recommendation is to keep them in archives for **ten (10) years**.	be duly substantiated and documented, also in light of the rights to privacy such individual has. Please note that there is a legal tension between the Dutch data protection rules (delete as soon as possible) and the need for such data for evidence in employment proceedings.
Ex-Employees records	**Seven (7) years** after the termination of employment.	Employee records should be kept at an address in the BVI for **not less than six (6) years** from the termination of employment.	**Fifty (50) years** from termination of employment for pay-rolls and documents related to the length of service and social insurance term, including employment contract, work-books (not received by the employee), journals, certificates, orders for appointment, reappointment, termination and long-term non-paid leave (more than thirty (30) days) and other similar documents that can serve as a basis for pension. For other data/records/documents related to ex-employees the retention periods mentioned above should be also applicable. <u>After expiry of the 50-year term, do not destroy these documents and/or</u>	**Three (3) years** from termination of employment.	No statutory retention period so UK position likely to be acceptable.	Permanently	No statutory retention period. Such data should not be retained for longer than is necessary for the purposes for which the data was collected. The Danish Data Protection Agency prescribes that employee records may be kept until **five (5) years** after the termination of employment. Such data can be kept longer if needed in order to e.g. comply with legal obligations or to defend or pursue a legal claim.	No statutory retention period so UK position likely to be acceptable (with exemption of the tax and social security records, cf. above). It is recommended to retain the complete personnel file for the applicable contractual forfeiture period or three years commencing from the end of the year when the employment has terminated (statutory limitation period for civil law claims). At least in case the employee requests deletion, one should consider blocking (*Sperrung*) according to Section 35 para 3 German Data Protection Act. Documents relating to company pension grant should be retained	No statutory retention period. However, in the event the document contains sensitive personal data or information pertaining to the candidate(s), the law mandates that a body corporate or a person on its behalf shall not retain such information for longer than it is required for the purposes for which the information may be lawfully used (the information collected shall be used for the purpose for which it has been collected) or the same is otherwise required under any law for the time being in force.	No statutory retention period. The default position applies: such data should not be retained for longer than is necessary for the purposes for which the data was collected. Please note that the French data protection authority (CNIL) has issued a recommendation not to retain such data for longer than the duration of employment. In practice, the Luxembourg data protection authority frequently adheres to the recommendations made by the CNIL. It is therefore recommended to destroy such data after termination of the employment contract, with the exception of data governed by specific rules (e.g. employment	No statutory retention period. The general rule is that such data should not be retained for longer than is necessary for the fulfilment of the purpose for which the data was collected. Malaysian law requires employers to keep information registers of their employees for not less than six (6) years.	Although according to Articles 516 and 804 of the FLL it is not necessary to hold files for more than a year, our recommendation is to keep them in archives for **five (5) years**.	Employee records must be kept for **seven (7) years** after the termination of employment. They may be kept longer if necessary in the interest of the company. This however needs to be duly substantiated and documented, also in light of the rights to privacy such individual has. Please note that there is a legal tension between the Dutch data protection rules (delete as soon as possible) and the need for such data for evidence in employment proceedings.

Document	Australia	British Virgin Islands (BVI)	Bulgaria	Canada	Cyprus	China	Denmark	Germany	India	Luxembourg	Malaysia	Mexico	Netherlands
			data before prior confirmation from the Legal Department.					until due date (retirement of employee).		contract – **ten (10) years**; accounting documents related to duration of employment – **three (3) years**; please also refer to the specific rules in the rows above).			

Document	Poland	Romania	Russia	Singapore	South Africa	Sweden	Switzerland	UK	Ukraine	USA[6] [USA 5]	Vietnam
Unsolicited application forms/CVs (not to be pursued)	The candidate's data should be kept as long it is necessary for particular requirement process. If the application was made without the particular requirement process, then he should be asked whether the CV can be kept for particular period of time (e.g. **two (2) months**) for new opening, otherwise it should be deleted. **Fifty (50) years** from termination of employment in case of successful candidates and when information was transferred to the employees' personnel file.	No statutory retention period.	Russian legislation doesn't contain definition of "unsolicited application forms/CVs". There are only restrictions according to personal data legislation: a candidate grants consent for personal data processing which is effective till its revocation by a candidate, but **no less than seventy five (75) years**.	No statutory retention period. Under the Singapore Personal Data Protection Act 2012 ("PDPA"), an organization must cease to retain personal data as soon as it is reasonable to assume that the purpose for which that personal data was collected is no longer being served by retention of the personal data; and retention is no longer necessary for legal or business purposes. We suggest that Luxoft retain the personal data for no longer than **six (6) months** unless necessary for legal or business purposes.	No statutory retention period. Records may not be retained for any longer than is necessary for achieving the purpose for which the information was collected unless required by law, LUXOFT GROUP requires the record for a lawful purpose, for purposes of a contract with the individual or the individual has consented to the retention of the record.	No statutory retention period. Personal data regarding rejected candidates must be deleted as soon as the information is no longer needed for the purpose for which the information was collected, i.e. when the recruitment process has been concluded (unless the candidate has consented that the information may be kept on file). However, in case of a possible dispute (e.g. on grounds of discrimination) the data may be stored for a period of two (2) years or if such dispute is initiated until the dispute is finally settled.	Documents to be returned to the applicant as soon as not necessary anymore (After three months at the latest documents should be deleted to follow the practice of the Government). If a candidate expressly requests deletion of their data, this should be done immediately.	**Nine (9) months** from date of receipt (unless candidate has agreed details should be kept on file). (Recommended period based on the fact that under the new employment tribunal process, it could take some time for the claim to be processed and so employers may not be made aware of the claims for much longer than it took previously).	For a period that does not exceed the time necessary for the purposes for which such data are being processed. In any case, personal data shall be processed in a format allowing the identification of individuals but no longer than prescribed by legislation on archives, which is **one (1) year** for the documents of candidates not accepted for employment.	**FED: One (1) to two (2) years** (depending on statute) from date hiring process is completed. If complaint is filed by applicant, then records must be kept until final disposition. **CA: Two (2) years** from date the records are created or received. If complaint is filed by applicant, then records must be kept until final disposition. **NY: Three (3) years** from date hiring process is completed. If complaint is filed by applicant, then records must be kept until final disposition. **TX: One (1) year** following receipt. **MI/WA:** No regulations so follow FED.	No statutory retention period. However, as the document arguably might contain personal information of the candidate/employee, privacy law suggests that those who collect or process such personal information may store it only for a period as agreed by the candidate/employee.

[6] Retention of HR records in the United States is governed by both federal (FED) and state law. Luxoft offices located in different states, and they may have different statutory requirements as indicated in this matrix. If the state and federal retention periods differ, employer must comply with the jurisdiction that requires the longest retention period. If your location has less than 50 employees, then Family Medical Leave Act (FMLA) does not apply, but other FED statutes may still be applicable. Due to its strict standards FMLA may nevertheless serve as a best practice in these cases. This matrix does not include local city ordinances that may apply.

Application Forms/CVs	The candidate's data should be kept as long it is necessary for particular requirement process. If the application was made without the particular requirement process, then he should be asked whether the cv can be kept for particular period of time (e.g. **two (2) months**) for new opening, otherwise it should be deleted. **Fifty (50) years** from termination of employment in case of successful candidates and when information was transferred to the employees' personnel file.	**Thirty (30) years** from the hiring date.	Russian legislation doesn't contain definition of "application forms/CVs". If application forms/CVs are taken from public source (Internet, social networks) – no need in candidates consent for personal data processing, but **no less than seventy five (75) years**.	No statutory retention period. Under the Singapore PDPA, an organization must cease to retain personal data as soon as it is reasonable to assume that the purpose for which that personal data was collected is no longer being served by retention of the personal data; and retention is no longer necessary for legal or business purposes. We suggest that Luxoft retain the personal data for no longer than **six (6) months** unless necessary for legal or business purposes.	**Three (3) years** from the date of the termination of employment.	No statutory retention period. In general such records may not be kept for a longer period than "necessary" with regard to the purpose of the processing. The applicable "necessary" retention period is dependent on the information recorded. If kept in the employees' personal files it may be kept at least until the termination of the employment. Please note that the retention period after the termination of the employment shall in no case be shorter than applicable statutory minimum retention periods (e.g. personal data processed for accounting purposes shall be stored for seven (7) years according to the requirements in the Swedish Accounting Act). Please note that the Swedish Data Protection Authority has provided recommended retention periods during which personal data may be stored. In general employee personal data should be deleted once the employment relationship has ended. However, data may be stored for as long as (i) there is a potential for a dispute between the company and the former employee, or (ii) the information is necessary with regard to administrative purposes e.g. to administer pension payments, issue work certificates or to provide references to other employers. In addition, the company may keep factual information for	No statutory retention period. Documents to be returned to the applicant as soon as the application process is over. (After three months at the latest documents shall be deleted to follow the practice of the Government). If a candidate expressly requests deletion of their data, this should be done immediately.	**Nine (9) months** after completion of the recruitment exercise to which they relate (unless the applicant has issued a complaint about the application process or decision). (Recommended period based on the fact that under the new employment tribunal process, it could take some time for the claim to be processed and so employers may not be made aware of the claims for much longer than it took previously). Information relating to successful candidates may, where relevant, be transferred to the employees' personnel file	For a period that does not exceed the time necessary for the purposes for which such data are being processed. In any case, personal data shall be processed in a format allowing the identification of individuals but no longer than prescribed by legislation on archives. According to legislation on archives, **seventy five (75) years** from termination of employment.	**FED: One (1) to two (2) years** (depending on statute) from date hiring process is completed. If complaint is filed by applicant, then records must be kept until final disposition. **CA: Two (2) years** from date the records are created or received. If complaint is filed by applicant, then records must be kept until final disposition. **NY: Three (3) years** from date hiring process is completed or, if hired, no less than **three (3) years** after termination of employment. If complaint is filed by applicant, then records must be kept until final disposition. **TX: One (1) year** following receipt. **WA/MI:** No regulations so follow FED.	Same as above.

Interview notes	The candidate's data should be kept as long it is necessary for particular requirement process. If the application was made without the particular requirement process, then he should be asked whether the cv can be kept for particular period of time (e.g. **two (2) months**) for new opening, otherwise it should be deleted. **Fifty (50) years** from termination of employment in case of successful candidates and when information was transferred to the employees' personnel file.	No statutory retention period.	Russian legislation doesn't contain definition of "interview notes".	No statutory retention period. Under the Singapore PDPA, an organization must cease to retain personal data as soon as it is reasonable to assume that the purpose for which that personal data was collected is no longer being served by retention of the personal data; and retention is no longer necessary for legal or business purposes. We suggest that Luxoft retain the personal data for no longer than **six (6) months** unless necessary for legal or business purposes.	**One (1) year** from the date of creation of the record or completion of the hiring process, whichever is later.	Please see comment on Application Forms/CVs above.	No statutory retention period. Documents to be deleted as soon as the application process is over. (After three months at the latest documents shall be deleted to follow the practice of the Government), If a candidate expressly requests deletion of their data, this should be done immediately.	**Nine (9) months** after the interview (either internal or external) (unless the candidate has made a complaint about the interview). (Recommended period based on the fact that under the new employment tribunal process, it could take some time for the claim to be processed and so employers may not be made aware of the claims for much longer than it took previously).	For a period that does not exceed the time necessary for the purposes for which such data are being processed. In any case, personal data shall be processed in a format allowing the identification of individuals but no longer than prescribed by legislation on archives. According to legislation on archives, **seventy five (75) years** from termination of employment.	**FED: One (1) to two (2) years** (depending on statute) from date hiring process is completed. If complaint is filed by applicant, then records must be kept until final disposition. **CA: Two (2) years** from date the records are created or received. If complaint is filed by applicant, then records must be kept until final disposition. **NY: Three (3) years** from date hiring process is completed or, if hired, no less than **three (3) years** after termination of employment. If complaint is filed by applicant, then records must be kept until final disposition. **TX: One (1) year** following receipt. **MI/WA:** No regulations so follow FED.	Same as above.

References given to a potential future employer	**Fifty (50) years** from termination but only when information was transferred to the employees' personnel file.	No statutory retention period.	Russian legislation doesn't contain definition of "references given to a potential future employer".	No statutory retention period. Under the Singapore PDPA, an organization must cease to retain personal data as soon as it is reasonable to assume that the purpose for which that personal data was collected is no longer being served by retention of the personal data; and retention is no longer necessary for legal or business purposes. We suggest that Luxoft retain the personal data for no longer than **six (6) months** unless necessary for legal or business purposes.	No statutory retention period. Records may not be retained for any longer than is necessary for achieving the purpose for which the information was collected unless required by law, LUXOFT GROUP requires the record for a lawful purpose, for purposes of a contract with the individual or the individual has consented to the retention of the record.	Please see comment on Application Forms/CVs above.	No statutory retention period so UK position likely to be acceptable.	**Six (6) months** from the date of issue.	For a period that does not exceed the time necessary for the purposes for which such data are being processed. In any case, personal data shall be processed in a format allowing the identification of individuals but no longer than prescribed by legislation on archives. According to legislation on archives, **seventy five (75) years** from termination of employment.	No per se statutory retention period so comply with UK standard.	Same as above.
Absence records showing incidence of sickness absence, annual leave and other approved and unapproved absence	**Fifty (50) years** from termination of employment but only when information was transferred to the employees' personnel file.	**Thirty (30) years** from the inception date of the documents.	Absence records showing incidence of sickness absence, annual leave – **five (5) years**. Long-term absence (including business trips, maternity leave, unpaid vacation etc.) – **seventy five (75) years.**	No statutory retention period. We suggest that records be kept for **seven (7) years** (i.e. the six year limitation period for contractual claims plus one year).	**Three (3) years** from the date of the termination of employment.	Please see comment on Application Forms/CVs above.	Data necessary to establish a work certificate to be retained **ten (10) years** from termination of employment.	**Three (3) years** from termination of employment.	For a period that does not exceed the time necessary for the purposes for which such data are being processed. In any case, personal data shall be processed in a format allowing the identification of individuals but no longer than prescribed by legislation on archives. According to legislation on archives, medical records and other documents of secondary importance are kept **three (3) years** from termination of employment, documents on granting and use of annual leave shall be retained for **one (1) year.**	**FED/MI/TX:** No less than **three (3) years** from date record is created. **CA/NY:** No less than **three (3) years** after termination of employment. **WA:** No regulations so follow FED.	Same as above.

Appraisals and performance reviews	**Fifty (50) years** from termination of employment but only when information was transferred to the employees' personnel file.	**Thirty (30) years** from the inception date of the documents.	**Seventy five (75) years.**	No statutory retention period. Under the Singapore PDPA, an organization must cease to retain personal data as soon as it is reasonable to assume that the purpose for which that personal data was collected is no longer being served by retention of the personal data; and retention is no longer necessary for legal or business purposes. We suggest that records be kept for **seven (7) years** (i.e. the six year limitation period for contractual claims plus one year).	**Three (3) years** from the date of termination of employment.	Please see comment on Application Forms/CVs above.	Data necessary to establish a work certificate to be retained **ten (10) years** from termination of employment.	**Six (6) months** from termination of employment.	For a period that does not exceed the time necessary for the purposes for which such data are being processed. In any case, personal data shall be processed in a format allowing the identification of individuals but no longer than prescribed by legislation on archives. According to legislation on archives, **seventy five (75) years** from termination of employment.	**FED/MI:** No less than **three (3) years** from date record is created. **CA/NY:** No less than **three (3) years** after termination of employment. **TX: One (1) year** following employee's last day of work. **WA:** No regulations so follow FED.	Same as above.
Records relating to promotion	**Fifty (50) years** from termination of employment but only when information was transferred to the employees' personnel file.	**Thirty (30) years** from the inception date of the documents.	**Seventy five (75) years.**	No statutory retention period. Under the Singapore PDPA, an organization must cease to retain personal data as soon as it is reasonable to assume that the purpose for which that personal data was collected is no longer being served by retention of the personal data; and retention is no longer necessary for legal or business purposes. We suggest that records be kept for **seven (7) years** (i.e. the six year limitation period for contractual claims plus one year).	No statutory retention period. We recommend that these records are retained for a period of **three (3) years** from the date of the termination of employment.	Please see comment on Application Forms/CVs above.	Data necessary to establish a work certificate to be retained **ten (10) years** from termination of employment.	**Six (6) months** from termination of employment.	For a period that does not exceed the time necessary for the purposes for which such data are being processed. In any case, personal data shall be processed in a format allowing the identification of individuals but no longer than prescribed by legislation on archives. According to legislation on archives, **seventy five (75) years** from termination of employment.	**FED/MI:** No less than **three (3) years** from date record is created. **CA/NY:** No less than **three (3) years** after termination of employment. **TX: One (1) year** following employee's last day of work. **WA:** No regulations so follow FED.	Same as above.

Reference provided by a former employer	**Fifty (50) years** from termination of employment but only when information was transferred to the employees' personnel file.	No statutory retention period.	Russian legislation doesn't contain definition of "references provided by a former employer".	No statutory retention period. Under the Singapore PDPA, an organization must cease to retain personal data as soon as it is reasonable to assume that the purpose for which that personal data was collected is no longer being served by retention of the personal data; and retention is no longer necessary for legal or business purposes. We suggest that Luxoft retain the personal data for no longer than **six (6) months** unless necessary for legal or business purposes.	No statutory retention period. Records may not be retained for any longer than is necessary for achieving the purpose for which the information was collected unless required by law, LUXOFT GROUP requires the record for a lawful purpose, for purposes of a contract with the individual or the individual has consented to the retention of the record.	Please see comment on Application Forms/CVs above.	No statutory retention period so same as UK.	**Six (6) months** from receipt.	For a period that does not exceed the time necessary for the purposes for which such data are being processed. In any case, personal data shall be processed in a format allowing the identification of individuals but no longer than prescribed by legislation on archives. According to legislation on archives, **seventy five (75) years** from termination of employment.	**FED/CA/MI/TX/WA:** No per se statutory retention period so comply with UK standard. **NY: Three (3) years** from date hiring process is completed or, if hired, no less than **three (3) years** after termination of employment. If complaint is filed by applicant, then records must be kept until final disposition.	Same as above.
Summary of record of service (including name, position held and dates of employment)	**Fifty (50) years** from termination of employment but only when information was transferred to the employees' personnel file.	**Thirty (30) years** from the inception date of the documents.	During the employment term of a candidate. Is immediately returned at the last day of employment.	No statutory retention period. Under the Singapore PDPA, an organization must cease to retain personal data as soon as it is reasonable to assume that the purpose for which that personal data was collected is no longer being served by retention of the personal data; and retention is no longer necessary for legal or business purposes. We suggest that records be kept for **seven (7) years** (i.e. the six year limitation period for contractual claims plus one year).	**Three (3) years** from the date of the termination of employment.	Please see comment on Application Forms/CVs above.	Data necessary to establish a work certificate to be retained **ten (10) years** from termination of employment.	**One (1) year** from termination of employment (unless the employee has agreed details should be kept on file).	For a period that does not exceed the time necessary for the purposes for which such data are being processed. In any case, personal data shall be processed in a format allowing the identification of individuals but no longer than prescribed by legislation on archives. According to legislation on archives, **seventy five (75) years** from termination of employment.	**FED/MI:** No less than **three (3) years** from date record is created. **CA/NY:** No less than **three (3) years** after termination of employment. **TX: One (1) year** following employee's last day of work. **WA:** Four (4) years following calendar year in which employment occurred.	Same as above.

Payroll and tax records	**Payroll – fifty (50) years** from making the files. **Tax records – ten (10) years** from the end of the tax year in which the tax obligation arose. **Five (5) years** for any social benefits documents from the transfer of the documents to the Social Security Office.	**Payroll – fifty (50) years** from the end of financial year in which they were made. **Tax records – thirty (30) years** from the inception date of the documents.	Payroll – **five (5) years**. n case of absence of personal accounts – **seventy five (75) years**. Payroll sheets for insurance premium transferred to Social Insurance Fund – **five (5) years**. Payroll correspondence – **five (5) years**.	Under the Companies Act, Goods and Service Tax Act, and Income Tax Act: • At least **seven (7) years**, for records relating to accounting periods ending before 1 January 2007; and • At least **five (5) years**, for records relating to accounting periods ending on or after 1 January 2007. We suggest that records be kept for **seven (7) years** (i.e. the six year limitation period for contractual claims plus one year).	**Five (5) years** from the date of submission of a tax return until the last day of the tax assessment period.	For a minimum of **seven (7) years**. The seven year retention period starts in the year following the expiry of the calendar year in which the accounting year (to which the information relates) was closed.	**Ten (10) years** from the end of the civil year.	**Six (6) years** from termination of employment.	For a period that does not exceed the time necessary for the purposes for which such data are being processed. In any case, personal data shall be processed in a format allowing the identification of individuals but no longer than prescribed by legislation on archives. **Payroll – ten (10) years** or **seventy five (75) years** in the absence of an order on appointment and change of a salary. **Tax records – ten (10) years** from the end of the tax year in which the tax obligation arose. Documents on payment of taxes and fees - **five (5) years**. .	**FED: Three (3) years** minimum from date record is created. Recommended six years given statute of limitations. **CA:** No less than **three (3) years** after termination of employment. Recommended four years given statute of limitations. **MI:** None, so follow FED. **NY:** Not less than **six (6) years** from date record is created. **TX: Four (4) years** after the date of the last payroll check (*see* Texas unemployment compensation statute) **WA:** Four (4) years following calendar year in which employment occurred.	• **Five (5) years** from the date of filing for accounting records not directly used for making entries in accounting books and financial statements; or • **Ten (10) years** from the date of filing for accounting records directly used for making entries in accounting books and financial statements, accounting books and annual financial statements.

Records relating to accident or injury at work	**Fifty (50) years** from making the files.	Records of individually monitored employee exposure to radiation – **forty (40) years** from the exposure date; shall be kept by occupational medicine entity agreed by the employer.	**Seventy five (75) years** for documents relating to scene of accident; if associated with major material damage and victims – **forever** (if occurred in scene of accident). If occurred in other entities - **five (5) years.**	**Five (5) years** under the Workplace Safety and Health Act. We suggest that records be kept for **seven (7) years** (i.e. the six year limitation period for contractual claims plus one year).	**Forty (40) years** from the date of the incident.	Please see comment on Application Forms/CVs above.	**Five (5) years** from date of incident.	**Three and a half (3.5) years** from date of incident.	For a period that does not exceed the time necessary for the purposes for which such data are being processed. In any case, personal data shall be processed in a format allowing the identification of individuals but no longer than prescribed by legislation on archives. E.g. documents (protocols, reports, conclusions) of harmful labour conditions, injuries, occupational diseases - **seventy five (75) years**; documents (reports, certificates, lists) of injury at the workplace – **ten (10) years**; acts on investigation of occupational diseases and poisonings – **forty five (45) years** etc.	**FED/NY/WA: Five (5) years** following the end of the calendar year that these records cover. [Note: NY Workers' Compensation Board Form C-2F ("Employer's First Report of Work-Related Injury/Illness") must be retained for 18 years. **CA/TX: Five (5) years** from date of incident. **MI:** None, so follow FED.	No statutory retention period. However, as the document arguably might contain personal information of the candidate/employee, privacy law suggests that those who collect or process such personal information may store it only for a period as agreed by the candidate/employee.
"Spent" disciplinary proceedings Warnings	**After one (1) year** of impeccable work.	**After one (1) year** of impeccable work.	**Three (3) years** for characteristics, certificates, memos for brining to disciplinary responsibility. **Five (5) years** for disciplinary penalty orders.	No statutory retention period. Under the Singapore PDPA, an organization must cease to retain personal data as soon as it is reasonable to assume that the purpose for which that personal data was collected is no longer being served by retention of the personal data; and retention is no longer necessary for legal or business purposes. We suggest that records be kept for **seven (7) years** (i.e. the six year limitation period for contractual claims plus one year).	**Three (3) years** from the date of the termination of employment.	No statutory retention period. In general to the extent records contain personal data such records may not be kept for a longer period than "necessary" with regard to the purpose of the processing. The applicable "necessary" retention period is dependent on the information recorded.	Data necessary to establish a work certificate to be retained **ten (10) years** from termination of employment.	**Six (6) months** for verbal warning and **twelve months** for written warnings.	For a period that does not exceed the time necessary for the purposes for which such data are being processed. In any case, personal data shall be processed in a format allowing the identification of individuals but no longer than prescribed by legislation on archives. E.g. documents on infringement of internal rules of conduct **one (1) year** from the date of issue.	**FED/MI:** No less than **three (3) years** from date record is created. **CA/NY:** No less than **three (3) years** after termination of employment. **TX: One (1) year** following employee's last day of work. **WA:** No regulations so follow FED.	Same as above.

Grievances	Same as UK.	**Thirty (30) years** from the registration date with the employer.	**Five (5) years.**	No statutory retention period. Under the Singapore PDPA, an organization must cease to retain personal data as soon as it is reasonable to assume that the purpose for which that personal data was collected is no longer being served by retention of the personal data; and retention is no longer necessary for legal or business purposes. We suggest that records be kept for **seven (7) years** (i.e. the six year limitation period for contractual claims plus one year).	**Three (3) years** from the date of the termination of employment.	No statutory retention period. In general to the extent records contain personal data such records may not be kept for a longer period than "necessary" with regard to the purpose of the processing. The applicable "necessary" retention period is dependent on the information recorded.	Data necessary to establish a work certificate to be retained **ten (10) years** from termination of employment.	**Six (6) months** after resolution of the grievance.	For a period that does not exceed the time necessary for the purposes for which such data are being processed. In any case, personal data shall be processed in a format allowing the identification of individuals but no longer than prescribed by legislation on archives. Documents on labour disputes - **five (5) year**.	**FED/MI:** No less than **three (3) years** from date record is created. **CA/NY:** No less than **three (3) years** after termination of employment. **TX: One (1) year** following employee's last day of work. **WA:** No regulations so follow FED.	Same as above.
Criminal Convictions	Same as UK. **Fifty (50) years** from termination of employment but only when information was transferred to the employees' personnel file.	No statutory retention period.	Statutory retention period is not specified.	No statutory retention period. Under the Singapore PDPA, an organization must cease to retain personal data as soon as it is reasonable to assume that the purpose for which that personal data was collected is no longer being served by retention of the personal data; and retention is no longer necessary for legal or business purposes. We suggest that records be kept no longer than it takes for convictions to become "spent" in accordance with the Registration of Criminal Act.	No statutory retention period. We recommend that these records are retained for a period of **three (3) years** from the date of the termination of employment.	In general it is prohibited for others than public authorities to process personal data concerning legal offences involving criminal offences, judgments in criminal cases, coercive criminal procedural measures or administrative deprivation of liberty, even under circumstances where consent is obtained from the data subject.	If related to the employment and necessary to establish a work certificate, it might be retained **ten (10) years** from termination of employment.	Upon [first annual update after] such convictions becoming "spent" under the Rehabilitation of Offenders Act 1974 unless, exceptionally information is retained to prevent re-employment.	For a period that does not exceed the time necessary for the purposes for which such data are being processed. In any case, personal data shall be processed in a format allowing the identification of individuals but no longer than prescribed by legislation on archives. No statutory retention period, so same as UK.	Criminal convictions are regulated by consumer reporting statutes. If applicant is not hired based on job-related criminal conviction, then follow applicant retention periods. If employee is terminated based on job-related criminal conviction, then follow post-termination personnel record retention period.	Same as above.

Ex-Employees records	**Fifty (50) years** from termination of employment (employees' personal records and other documentation related to the employment relationship stored in hard copies**)**, payroll lists, carts with remuneration, or other evidence that can be basis for pension stored in hard copies); **Fifty (50) years** from development of documents related to employees' payroll files.	Retention periods mentioned above shall be also applicable for ex-employees.	**Seventy five (75) years.**	No statutory retention period. Under the Singapore PDPA, an organization must cease to retain personal data as soon as it is reasonable to assume that the purpose for which that personal data was collected is no longer being served by retention of the personal data; and retention is no longer necessary for legal or business purposes. We suggest that records be kept for **seven (7) years** (i.e. the six year limitation period for contractual claims plus one year).	**Three (3) years** from the date of the termination of employment.	It depends on the information included in the records. No statutory retention period. In general to the extent records contain personal data such records may not be kept for a longer period than "necessary" with regard to the purpose of the processing. The applicable "necessary" retention period is dependent on the information recorded. Please note that the retention period shall in no case be shorter than applicable statutory minimum retention periods (e.g. personal data processed for accounting purposes shall be stored for seven (7) years according to the requirements in the Swedish Accounting Act). Please note that the Swedish Data Protection Authority has provided recommended retention periods during which personal data may be stored. In general employee personal data should be deleted once the employment relationship has ended. However, data may be stored for as long as (i) there is a potential for a dispute between the company and the former employee, or (ii) the information is necessary with regard to administrative purposes e.g. to administer pension payments or to provide references to other employers. In addition, the company may keep factual information for a longer period (as long as the	Data necessary to establish a work certificate to be retained **ten (10) years** from termination of employment.	**Archived for six (6) years** and then securely destroyed.	For a period that does not exceed the time necessary for the purposes for which such data are being processed. In any case, personal data shall be processed in a format allowing the identification of individuals but no longer than prescribed by legislation on archives. According to legislation on archives, **seventy five (75) years** from termination of employment.	Depends on type of record. Generally, archive personnel records for **three (3) years** and then securely destroy. Payroll records may have a longer retention period. **WA**: Requires retention of the following information for **four (4) years** following calendar year in which employment occurred: name, Social Security number, dates of employment, basis upon which wages are paid, location of services, days worked, number of hours worked each day, total gross pay period earnings, specific sums withheld from earnings and purpose of withholding, cause for discharge or separation.	Same as above.

SUPPLEMENTARY DOCUMENT 4: SAMPLE DATA PROCESSOR WORDING

Set out below is some precedent data processor wording which should be added to contracts where a LUXOFT GROUP entity is appointing a service provider who will be processing personal data on behalf of the respective LUXOFT GROUP entity (e.g archive companies, hosting or support providers). The clauses have been drafted on the assumption that they will be included in a longer contractual document. These have been drafted to comply with the provisions relating to processors set out in the European Data Protection Directive (Directive 95/46/EC). **[China 14]***)* respectively the EU General Data Protection Regulation (EU) 2016/679 ("**GDPR**") upon applicability.. **[Malaysia 14] [South Africa 10] [Singapore 8]**.

Additional provisions may be required where the LUXOFT GROUP entity, whose data is being processed, is based in Canada, Germany, Luxembourg, Poland, South Africa, Sweden or Switzerland. In this situation, please speak to the Data Protection Officer before using these clauses. **[India 2]**

1 Data Protection

1.1 The parties' attention is drawn to Directive 95/46/EC of the European Parliament and any legislation and/or binding regulations implementing them or made in pursuance of them (all referred to together as the "Data Protection Requirements"). **[Netherlands 5] [Switzerland 1 and 7]**

1.2 It has been agreed between the parties that the Service Provider [LUXOFT entity processing data on behalf of other LUXOFT Group entity] will under contract to and on behalf of [insert relevant LUXOFT GROUP entity] ("**LUXOFT Entity**") process certain personal data of Controller ("**LUXOFT Entity's Personal Data**"). **[Poland 8]** The Service Provider acknowledges that LUXOFT Entity is the data controller in respect of LUXOFT Entity's Personal Data that the Service Provider processes in the course of providing services for LUXOFT Entity, and that the Service Provider is the data processor in respect of LUXOFT Entity's Personal Data.

1.3 The Service Provider agrees that it shall: **[South Africa 11]**

(a) only (i) carry out processing of LUXOFT Entity's Personal Data in accordance with LUXOFT Entity's instructions as set out in this Agreement and in particular as set out in Annex 1 or as those instructions may be amended from time to time and (ii) comply with instructions from LUXOFT Entity to rectify, erase and/or block LUXOFT Entity's Personal Data; **[China 15]**

(b) agree with LUXOFT Entity and implement appropriate technical and organizational measures to protect LUXOFT Entity's Personal Data against unauthorised or unlawful processing and accidental destruction or loss, including without limitation the measures set out in Annex 2 or such other measures as may be agreed between the parties;

(c) use all reasonable endeavours to advise LUXOFT Entity if, in the light of new technology and methods of working, LUXOFT Entity should consider revising the security methods specified in Annex 2;

(d) not sub-contract any processing of LUXOFT Entity's Personal Data without the prior written consent of LUXOFT Entity; [***Note: please speak to the Data Protection Officer if sub-processing is required.]*** **[India 2, India 6 and India 7]**

(e) immediately refer to LUXOFT Entity any requests, notices or other communication from data subjects, data protection authorities or any other law enforcement authority, for LUXOFT Entity to resolve;

(f) at no additional cost, provide such information to LUXOFT Entity as LUXOFT Entity may reasonably require, and within the timescales reasonably specified by LUXOFT Entity, to allow LUXOFT Entity to comply with the rights of data subjects, including subject-access rights, or with notices served by any data protection authority;

(g) **[only if LUXOFT Entity is situated in the EU/EEA or in Switzerland:]**not transfer any of LUXOFT Entity's Personal Data outside of the European Economic Area without the prior written consent of LUXOFT Entity; [***Note: please speak to the Data Protection Officer if a transfer of data is required.]*** **[Australia 11] [China 15] [Russia 3] [Singapore 3] [Switzerland 1][India 2, India 6 and India 7]**

(h) represent and warrant that its collection, access, use, storage, disposal and disclosure of LUXOFT Entity's Personal Data does and will comply with all applicable federal, state, provincial, local, and foreign privacy and data protection laws, as well as all other applicable regulations and directives; and

(i) on the termination of this Agreement and at the choice of LUXOFT Entity, return all of LUXOFT Entity's Personal Data to LUXOFT Entity or destroy all of LUXOFT Entity's Personal Data and certify to LUXOFT Entity that it has done so, unless prevented from doing so by applicable laws. In that case, the Service Provider warrants that it will guarantee the confidentiality of LUXOFT Entity's Personal Data and will not actively process such personal data anymore.

1.4 The Service Provider shall, at no additional cost, keep or cause to be kept full and accurate records relating to all processing of LUXOFT Entity's Personal Data on behalf of LUXOFT Entity, including but not limited to the records specified in Annex 3, and shall, upon reasonable notice, grant LUXOFT Entity and its auditors and agents, a right of access to and to take copies of such records in order to assess whether the Service Provider has complied with the provisions of Clause [1.3]. The Service Provider shall, upon reasonable notice, allow LUXOFT Entity and its auditors and agents access to premises and other materials and to its personnel and shall provide all reasonable assistance in order to assist LUXOFT Entity and its auditors and agents in exercising its audit rights under this Clause. Service Provider's obligations under this Clause shall continue throughout the Agreement and for a period of six (6) years thereafter.

ANNEX 1: INSTRUCTIONS

This should include any specific instructions with which the Service Provider is required to comply (for example, using specific fair-obtaining notices).

ANNEX 2: SECURITY MEASURES

This should list any agreed security measures here – we have set out some examples below: **[Bulgaria 9] [India 8] [Poland 9] [Sweden 9]**

1. Access control to premises and facilities

Unauthorized access (in the physical sense) must be prevented.
Technical and organizational measures to control access to premises and facilities, particularly to check authorization:

☒ Access control system
☒ ID reader, magnetic card, chip card
☒ (Issue of) keys
☒ Door locking (electric door openers etc.)
☒ Surveillance facilities
☒ Alarm system, video/CCTV monitor
☒ Logging of facility exits/entries.

2. Access control to systems

Unauthorized access to IT systems must be prevented.
Technical (ID/password security) and organizational (user master data) measures for user identification and authentication:

☒ Password procedures (incl. special characters, minimum length, change of password)
☒ No access for guest users, no anonymous accounts
☒ Access to systems centrally managed and restricted to approval by both personnel management and system owner.

3. Access control to data

Access through IT systems outside the allocated access rights must be prevented.
Requirements-driven definition of the authorization scheme and access rights, and monitoring and logging of accesses:

☒ Differentiated access rights (profiles, roles, transactions and objects)
☒ Access rights defined according to duties and least privilege concepts
☒ Log of user access via IT systems.

4. Disclosure control

Aspects of the disclosure of personal data must be controlled: electronic transfer, data transport, transmission control, etc.

Measures to transport, transmit and communicate or store data on data media (manual or electronic) and for subsequent checking:

☒ All data is transferred via wholly-owned private network
☒ Encryption/tunneling (VPN = Virtual Private Network) for remote access, transport and communication of data.
☒ Prohibition of use of portable media.

5. Input control

Full documentation of data management and maintenance must be maintained.
Measures for subsequent checking whether data have been entered, changed or removed (deleted), and by whom:

Example:
☒ Systems log user activities according to the data importer's security logging standard.

6. Job control

Commissioned data processing must be carried out according to instructions.
Measures (technical/organizational) to segregate the responsibilities between the data exporter and the data importer:

☒ Unambiguous wording of the contract
☒ Formal commissioning (request form)
☒ Criteria for selecting the data importer
☒ Monitoring of contract performance.

7. Availability control

The data must be protected against accidental destruction or loss.
Measures to assure data security (physical/automated):

☒ Backup procedures
☒ Uninterruptible power supply (UPS)
☒ Remote storage
☒ Anti-virus/firewall systems.

8. Segregation control

Data collected for different purposes must also be processed separately.
Measures to provide for separate processing (storage, amendment, deletion, transmission) of data for different purposes:

Examples:
☒ Restriction of access to data stored for different purposes according to business function of staff.
☒ Segregation of business systems for different purposes
☒ Segregation of testing and production environments.

This should also include any policies or procedures adopted by the Service Provider that influenced LUXOFT Entity in its selection of the Service Provider and with which LUXOFT Entity requires the Service Provider to comply during the contract. For example, if LUXOFT Entity was influenced by the fact that the Service Provider meets the British Standards Institute data security standard, ISO/IEC 27001, then this should be referenced here.

The Act requires a data controller to choose a data processor that provides "sufficient guarantees" in relation to security and to take reasonable steps to ensure compliance with these security measures. One way in which LUXOFT Entity can take steps to ensure compliance is to list such security measures in the contract, so that, for example, there is an ongoing obligation on the data processor to meet ISO/IEC 27001.

9. Training

Service Provider must adopt the necessary measures to ensure that its staff are aware of security standards and privacy laws. Therefore staff of [*Service Provider*] will receive regular training on the application of privacy laws and security standards.

10. Audits

Service Provider must carry out audits to ensure that the measures set out in this document are complied with.

ANNEX 3: RECORDS

List any records to be kept by the Service Provider and the ways in which they will be made available to LUXOFT Entity (e.g. regular despatch, LUXOFT Entity's right of entry on the Service Provider's premises, etc.).

ANNEX B: SALES AND PROCUREMENT DEPARTMENTS

TRANSPARENCY

You should always ensure that LUXOFT GROUP is transparent about the use of personal data of business contacts.

SECURITY

LUXOFT GROUP entities acting as processor

You should always ensure that appropriate confidentiality and data protection clauses are included in contracts that you negotiate with customers. For example, it may be that a LUXOFT GROUP entity is actually processing personal data on behalf of a customer (e.g. where it is providing support and maintenance services which require access to a customer's database). In this case, it is for the customer to comply with the relevant data protection laws and to satisfy themselves that LUXOFT GROUP entity's procedures are adequate. It is important to ensure that standard language is included where required. Please contact the Data Protection Officer if you have any questions regarding the use of such wording. **[Australia 12] [Canada 6] [India 2China 14] [Malaysia 14 and Malaysia 3] [Netherlands 5] [South Africa 12]**

TRANSFERS

Any new requests to transfer personal data outside your own jurisdiction or to change the purpose of such transfers should only be done with the approval of the appropriate Data Protection Officer. **[India 2, India 6 and India 7][China 3] [Malaysia 2] [South Africa 3]**

[China 5]

ANNEX C: INFORMATION TECHNOLOGY DEPARTMENT

LAWFUL PURPOSES

New Uses — Use of data for a new purpose, can also affect LUXOFT GROUP's filings with data protection authorities (e.g. new IT applications or system developments). IT Staff should check that the relevant Department making the request has consulted the Data Protection Officer, if they wish to use personal data for a new purpose. **[India 2 and India 3] France 6] [Malaysia 3] [South Africa 8]**

DATA QUALITY

Test Data — Where live data is used for test purposes (if at all necessary), such data should where possible be anonymised prior to any such testing.

Data Review — Datasets should be reviewed regularly to ensure data is classified in line with Rules on Company information treatment by employees, Information Security Manual as well as to identify duplicate records, synchronise data, simplify access and streamline databases.

SECURITY

The Information Technology Department is responsible for assessing the Information Technology requirements to ensure appropriate security and will consult with the other Departments where appropriate. Much of this detail is set out in the Information Security Manual, Security Incident Management and related policies which should be consulted in addition to this document.

The Information Technology Department is responsible for reclaiming any IT equipment from staff who leave and ensuring that any hard drives are wiped.

The Information Technology Department is responsible for ensuring that all laptops and other portable media are encrypted. **[Netherlands 5]**

TRANSFERS

Where any system development or change in the IT services is planned (e.g. relocating data centres, changing IT applications or service providers, adopting new IT solutions and technologies) which may result in a transfer of data, you must seek the input of the appropriate Data Protection Officer. **[India 2, India 6 and India 7] [China 3] [Malaysia 3] [South Africa 3]**

RIGHTS

The Information Technology Department should action any requests from other Departments to update or correct information held in the databases managed by the Information Technology Department (to the extent that the Departments do not have the appropriate editing rights). **[Sweden 1] [China 5]**

ANNEX D: FACILITIES

DATA PROTECTION SAFEGUARDS

LAWFUL PURPOSES

Requests to disclose data

If you receive a request to forward personal data to a third party such as the police: you should first check with the Head of Personnel Department if it relates to an employee (current or former) or with the Data Protection Officer. They will determine if the release of this data would breach data protection legislation. **[India 2 and India 6][Malaysia 3] [South Africa 8]**

TRANSPARENCY

If data is collected about employees and / or visitors who access a LUXOFT GROUP entity's premises (e.g. when using a card system): notice about how LUXOFT GROUP uses this information should be included in an employee privacy notice. Save for the use of CCTV, it is not necessary to give notice to visitors as long as LUXOFT GROUP's use of their data is likely to be for expected purposes. **[Australia 13] [Bulgaria 10] [France 12] [China 16] [Malaysia 13] [Singapore 9]**

Notice of CCTV use

If you are responsible for monitoring the security of LUXOFT GROUP's premises by use of CCTV cameras (especially in reception areas and car parks): you will be responsible for ensuring that the CCTV is drawn to the attention of employees, visitors and others who may be recorded by positioning prominent notices wherever the CCTV is used.

Before CCTV is introduced into new areas, you must carry out an impact assessment to ensure that there is a business need for monitoring which justifies its use and to ensure that the monitoring is carried out with the minimum of intrusion, and in accordance with any local law requirements. **[Australia 14] [Cyprus 13] [Germany 4] [Luxembourg 9] [Romania 5] [Sweden 10]**

Sensitive Personal Data

If a specific investigation by Facilities requires the processing of sensitive personal data (e.g. if an employee is suspected of criminal activities and CCTV is used to watch that specific individual for evidential purposes), you should seek prior approval from the Data Protection Officer. **[Bulgaria 11] [IndiaChina 2 and India 7] [Malaysia 3]**

RETENTION

If CCTV images are stored, this will be for a maximum period of 30 days. **[China 17]**

Visitor registers should be destroyed 3 years after the visitor has been to the building. **[Australia 15] [China 17] [Cyprus 14] [Malaysia 15] [Singapore 10] [Sweden 11]**

DATA QUALITY

You should ensure that there is a clear and foreseeable need for information collected about individuals. For example, CCTV should not be focussed on other non-LUXOFT GROUP private property or on public spaces such as streets. **[Malaysia 16]**

SECURITY

If access to and movement around some of LUXOFT GROUP's premises is monitored for security purposes: system access should be checked from time to time to ensure that there are no suspicious movements. **[Netherlands 5]**

RIGHTS

All requests from individuals to see their data (e.g. request for CCTV images) should be promptly forwarded to the Personnel Department (for employees) and to the Data Protection Officer in other situations. However, these Departments may require you to provide certain information in response to the requests. It is important that CCTV images are kept in a format that enables them to be provided in response to a request, provided that they have not already been deleted. **[Malaysia 17] [China 5]**

COUNTRY APPENDICES:

1. AUSTRALIA

1. Personal information pursuant to the Privacy Act 1988 (Cth) (the "Privacy Act") means information or an opinion about an identified individual or an individual who is reasonably identifiable whether the information or opinion is true or not and whether the information or opinion is recorded in a material form or not. "Individual" means a natural person. Entities must comply with the Australian Privacy Principles ("APPs") which are specified in a schedule to the Privacy Act.

2. In Australia there is no requirement to notify the processing of data to any data protection authority.

3. Sensitive information under the Privacy Act also includes membership of professional or trade association, membership of a political association, criminal record, genetic information about an individual that is not otherwise health information or biometric information that is used for the purpose of automated biometric verification or biometric identification or biometric templates. Sensitive information can only be collected with the individual's consent and if the information is reasonably necessary for one or more of the entity's activities, subject to limited exceptions specified in APP 3.

4. In Australia there is an employee record exemption which means that a record of personal information relating to the employment of an employee which is collected by an employer of that employee is exempt from the provisions of the Privacy Act. Examples of such personal information include terms and conditions of employment, the employee's personal and emergency contact details, the employee's performance or conduct, the employee's salary or wages. On this basis, transparency with respect to an employee record is not a requirement under the Privacy Act, however, the Fair Work Act 2009 (Cth) regulates the handling and access to employee records. In addition, where an entity proposes to disclose personal information or sensitive information of an employee to a third party or an associated entity overseas, the requirements of the Privacy Act would apply. It should be noted that job applicants and prospective employees do not fall within the employee records exemptions and are covered by the Privacy Act.

5. In Australia, when an entity collects personal information from an individual, it must inform the individual if it is likely to disclose the data outside Australia and, if practicable, to specify the countries where it is likely to be disclosed.

6. There are no specific exceptions to requirements for transparency and notification for business contact information. If it is not practicable to provide the prescribed information at the time of collecting information, the entity must provide information that is reasonable in the circumstances as soon as practicable after collecting the information.

7. The principles set out in section 4.6 are consistent with the Privacy Act and APP 8 in relation to cross-border disclosure of personal information outside Australia. Before an entity discloses personal information about an individual to an overseas recipient, including an associated or group entity, the entity must either take reasonable steps to ensure that the overseas recipient does not breach the Privacy Act or expressly inform the individual that if he or she consents to the disclosure of information the entity will not need to take reasonable steps to ensure that the overseas recipient does not breach the Act and after being so informed the individual consents to the disclosure. Staff should seek the input of the Data Protection Officer if you are not sure whether a data transfer agreement is in place to facilitate the transfer of personal data out of Australia to a third party or country.

8. Criminal records are considered sensitive information for the purposes of the Privacy Act. See note 3. In addition, while not prohibited, requesting criminal offence data can result in the risk of allegations of discrimination if it is not relevant to the position.

9. Information that forms part of an employee record is exempt from the provisions of the Privacy Act. However, an employee has the right to access certain employee records under the Fair Work Act 2009 and associated regulations. In the case of job applicants or candidates, where the individuals do not become employees, the information does not fall within the employee record exemption and accordingly is subject to the Privacy Act and individuals have a right to request to access such information.

10. In some states, monitoring of computer systems and emails and by CCTV may require specific notice periods, and in some cases consent, from employees under workplace surveillance legislation.

11. The agreement should specify that consent is required before the Service Provider transfers any Personal Data outside Australia.

12. The Privacy Act does not distinguish between data controllers and data processors and all parties that collect or hold personal information are bound by the requirements of the Privacy Act. Customer contracts should include appropriate warranties and indemnities from customers that the customer has obtained all relevant permissions, provided notifications and complied with the relevant privacy laws when collecting personal information provided to the LUXOFT GROUP entity for processing.

13. Personal data collected from visitors is subject to the notification requirements under the APPs. We recommend that visitors are provided with purpose notification language prior to the LUXOFT GROUP collecting, using or disclosing their personal data when they visit the premises.

14. In addition to notification requirements under the Privacy Act, workplace surveillance laws in some states require specific notice periods or consent before surveillance of employees commences.

15. Personal information must be destroyed or de-identified if it is no longer needed for a purpose permitted by the APPs and it is not required to be retained under an Australian law or court or tribunal. Therefore the 3 year period must be justified.

2. BULGARIA

1. Bulgarian law does not specify that personal data relate to *living* individuals. Any information relating to an identified or identifiable natural person who can be identified, directly or indirectly, will be considered personal data regardless whether the data subject is dead or alive.

2. The application of the legitimate interests as lawful grounds for personal data processing is very restricted. Although Bulgarian law lists the legal interests among the grounds for data processing, in practice most of the data controller's legitimate interests will not be considered to prevail the interests of the individuals concerned. Usually, the applicable legal grounds for lawful data processing are (1) the data subject's consent; (2) the necessity of the processing for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; and (3) compliance with legal obligations.

3. Data concerning human genome is also explicitly defined as sensitive data under Bulgarian law.

4. It is also necessary to provide information about the representative of the data controller and the categories of data which will be processed.

5. According to Bulgarian law this information should be provided. However, in practice this is usually not observed.

6. In Bulgaria, generally, employers shall not collect details about illnesses (only absence information), except in cases where such collection and processing of data concerning data subjects' health is necessary for compliance with obligations under labour legislation. If a data controller processes sensitive date, a prior permission by the Bulgarian DPA is required.

7. The use of data for a new purpose may also require data subjects' consent.

8. The confidentiality of the correspondence (including emails) is protected by the Constitution of the Republic of Bulgaria. The employer cannot read emails if it knows that it concerns private matters. Since there is no specific regulation on work emails, it is highly recommendable to ensure that employees are aware that they cannot use their work email addresses for private purposes and to explicitly prohibit such a use.

9. Under Bulgarian law, each data controller should carry out an impact assessment and on the basis of this impact assessment should determine the respective level of protection of the processed personal data. Depending on the determined level of protection, the data controller should implement respective minimum technical and organizational measures for protection of the personal data. For this purpose the data controller should adopt special Internal Rules (Instruction) on the technical and organizational measures for protection of the personal data.

10. Bulgarian law does not provide for special exception regarding the information obligations of the data controller in cases of use of CCTV.

11. This is prohibited by Bulgarian law. The employer is not allowed to investigate its employees. In case of any suspicions of criminal activities the employer should contact the competent authorities.

3. CANADA

1. In Canada (Province of Quebec), personal data should generally be collected from the individual concerned, except with the individual's consent or as authorized by law. If the source of the information is a legal person (e.g. a company), a mention to this effect should be included in the file. Please speak to the Data Protection Officer before collecting personal data from a third party without the individual's consent.

2. Personal health information and financial information is generally considered to be sensitive data in Canada.

3. In Canada (Province of Quebec), when the LUXOFT GROUP collects personal information from an individual, it must, when establishing a file on that individual, also inform the individual of the location where the file will be kept.

4. In Canada (Province of Alberta), when the LUXOFT GROUP entity uses a service provider (including an affiliate) outside Canada to collect, use, disclose or store personal data for or on behalf of the entity, it must include, in its policies and practices relating to processing of personal data, information regarding the countries outside Canada in which the collection, use, disclosure or storage is occurring or may occur, and the purposes for which the service provider outside Canada has been authorized to collect, use or disclose personal information for or on behalf of the organization. Written information about these policies and practices must be made available on request.

5. It is usually not permitted to collect criminal conviction data unless the job specifically requires it (e.g. financial crimes for a cashier).

6. Prescribed consent and content requirements apply under Canadian anti-spam legislation when sending commercial electronic messages that have a promotional purpose as one of their purposes to an email address. Please speak to the Data Protection Officer before sending such messages.

4. CHINA

1. “Personal Data" or "Personal Information" under the China Cyber Security Law and other applicable laws and regulations governing the protection of personal information in China is defined as all kinds of information which can be used, either alone or together with other information, to identify a natural person's personal identity, including but not limited to name, date of birth, identification numbers, personal biometric information, address, telephone numbers, account number and passwords.

2. In China, there is no separate definition of "sensitive personal data" under applicable laws and regulations. A Guideline (Information Security Technology – Guidelines for Personal Information Protection within Information System for Public and Commercial Services" issued by the State Administration of Standardisation provide that sensitive data such as personal ID card number, mobile number, data relating to race, political affiliation, religion, genetics and fingerprint are regarded as sensitive data, and specific requirements e.g. express consent should be obtained for the use and processing of sensitive data. However, the Guidelines do not have the force of law and are not legally binding.

3. Transfer of personal information to jurisdictions outside of China is generally regarded as a type of "use" of personal information and would be subject to notification and consent requirements. In particular, the consent of data subjects must be obtained. In addition, it should be noted that the PRC State Secret Law expressly prohibits information that constitutes "state secret" to be transferred outside of the PRC without the approval of the National Administration for the Protection of State Secrets. The term "state secret" is widely defined as matters which have a vital bearing on state security and national interests. Further, the Cyber Security Law imposes restrictions on cross-border transfer and obligations on security assessments which may be relevant to transfer of data by LUXOFT GROUP out of China. The exact requirements, and whether the requirements will be applicable to LUXOFT GROUP, will depend on implementation rules and regulations to the Cyber Security Law which are pending. LUXOFT GROUP should monitor the legal developments in this regard prior to conducting any transfer of personal information outside of China.

4. In China, there is no local data protection authority and no notification obligation on processing of personal data to any regulator. There is no requirement to appoint a Data Protection Officer.

5. In China, processing of personal data is subject to obtaining consent from the data subjects. There is no legitimate interest exception, and processing for compliance with legal obligation is not a ground for not obtaining consent.

6. The applicable data protection laws and regulations are silent on whether express or implied consent is required. In practice, it would be prudent for LUXOFT GROUP to obtain express consent where possible.

7. There are no specific exceptions to requirements for transparency, notification and consent for business contact information.

8. Data retention obligations are subject to applicable provisions of laws and regulations relating to data retention of specific data. There is no general obligation not to retain personal data for longer than necessary for the purposes for which the data was collected.

9. Where there is security breach, LUXOFT GROUP has additional obligations to report the breach to the relevant competent departments under the Cyber Security Law. LUXOFT GROUP should set up internal procedures for ensuring that such reporting obligations are met.

10. There is no legal requirement to enter into agreements similar to the European Commission approved agreements regulating transfer of data within LUXOFT GROUP of companies.

11. There is no legal right available to individuals in China to appeal or object to the use of automated decisions to take decisions about them.

12. Consent of employees is required prior to conducting any employee monitoring.

13. As indicated in (5) above, processing of personal data is subject to obtaining consent of data subjects, and not just notification. The Sample Privacy Notice For Employees should include a proviso that LUXOFT GROUP processes personal data subject to obtaining consent from the employees. An additional consent at the end of the Notice should specifically refer to consent for the use of personal data for the processing contemplated in the Notice.

14. There is no distinction under applicable data protection laws and regulations between a data user/controller and a data processor. Data processors who process personal data are directly subject to the data protection obligations under applicable law and regulations. This does not prevent data controller/user to enter into

contractual obligations on data processors as has been done in Supplementary Document 4. However it should be noted that this does not relieve the obligations on the LUXOFT GROUP as data transferor.

15. As indicated in (3) above, processing of personal data in China is subject to the requirement to obtain consent from relevant individuals. An additional obligation should be imposed to Clause 1.3 of the Supplementary Document 4 to include an obligation on the Service Provider to assist LUXOFT Entity obtain all consent necessary regarding the processing or use (including transfer) of LUXOFT Entity's Personal Data.

16. There is no consent exception for visitors under applicable laws and regulations on data protection in China. Visitors should be provided with purpose notification language and their consent obtained prior to the Company collecting, using or disclosing their personal data when they visit the premises.

17. There is no prescribed statutory retention period in respect of CCTV images and visitor records.

5. CYPRUS

1. 4.1.2 should be amended as follows (amendments printed in italic): Generally, staff may process personal data (other than sensitive personal data) (1) where this is necessary for LUXOFT GROUP's legitimate interests (as defined by local law), provided this does not cause unreasonable prejudice to the interests of the individuals concerned *and provided that LUXOFT GROUP's interests are not overridden by the interests for fundamental rights and freedoms of the data subjects requiring protection under the European Data Protection Directive and Cyprus local law implementing the same* and (2) where processing is necessary to comply with a legal obligation.

2. In Cyprus, the commission or alleged commission of any criminal offence, criminal prosecution and criminal convictions are sensitive personal data.

3. If personal data are transferred out of the EEA or Switzerland, the permission of the Cyprus Personal Data Commissioner will have to be obtained.

4. In Cyprus you cannot collect details about illnesses unless you obtain the data subject's consent. You can collect details about the health/ illnesses /medical condition without the data subjects consent if the following conditions are met:
   (i) Data are processed by a health professional who is subject to obligations of professional secrecy; and
   (ii) Processing is absolutely required for medical purposes, in order to prevent illnesses, diagnose illnesses and treat illnesses at working places.
   In addition, sickness records should be kept separately from other records containing personal data.

5. You must inform employees of the purpose of collection / processing of such data.

6. It is not usually permitted to collect criminal conviction data unless the job specifically requires it and you must inform the employees in advance / prior to collection of the data of the purpose of collection. Collection of such data must be made according to the provisions of the Cyprus Police Law, Law No. 73(I)/2004 (which provides that excerpt of criminal record kept by the Cyprus police may be given only to the data subject or to third parties to which the data subject has provided authorisation to obtain the excerpt of his/ her criminal record).

7. You must explain to unsuccessful applicants if you want to keep CVs on file for future use and CVs should only be retained if the applicant gives explicit consent.

8. Notes may be considered as personal data and be subject to the same protective regime as personal data.

9. You need explicit consent from employees to send to them direct marketing material.

10. Employees have a right to be informed in advance of the purposes of disclosing personal data to third parties, the personal data to be disclosed and the identity of the recipient third parties of such data. You may also be required to obtain employees' consent. LUXOFT GROUP may disclose freely personal data to third parties (without the data subject's consent) if LUXOFT GROUP has a legal obligation to disclose this information or information is required for legal proceedings or in connection with the prevention or detection of crime.

11. Employees must be notified in ALL circumstances of the purpose, type and duration of the monitoring before monitoring commences. Secret monitoring is not permissible.

12. The Employer cannot read / have access to the content of personal emails of employees and personal phone calls of employees. Emails which are marked as personal should not be read even in exceptional circumstances. LUXOFT GROUP may prohibit the use of its email systems for personal use by its employees. LUXOFT GROUP may adopt a policy for the use of internet and telephone specifying the meaning of the terms business use and personal use.

13. Before CCTV is introduced you must seek guidance from the Data Protection Officer. Employees must be notified in all circumstances of the purpose and duration of monitoring before monitoring commences. Secret monitoring is not permissible.

14. Retention period of 3 years may be considered as excessive under Cyprus law.

6. DENMARK

1. The Danish Law on Processing of Personal Data ("**PDA**") does not restrict the definition of personal data to *living* individuals. Any information relating to an identified or identifiable natural person who can be identified, directly or indirectly, will be considered as personal data regardless whether the data subject is dead or alive.

2. Personal data, which is processed, must be relevant and sufficient and limited to what is necessary in relation to the purposes for which it is processed.

3. Under the PDA a data subject has the right to request access, to object to the processing and to request the controller to correct, block or erase such personal data that has not been processed in accordance with Danish law.

4. Processing of semi-sensitive and sensitive personal data, cf. note 6, requires an authorization from the Danish Data Protection Agency ("**DPA**"). The PDA does not require a data protection officer.

5. Under the PDA the data controller may process ordinary personal data when for instance the processing is necessary to pursue a legitimate interest of the controller and this interest is not overridden by the interests of the data subject.

6. In Denmark information about criminal offences, significant social problems and other purely private matters (other than those mentioned as sensitive personal data) are considered as semi-sensitive personal data. Significant social problems are for instance information about social benefits. Other purely private matters are for instance family disputes, adoption, suicide, separation and severe violation of terms of employment.

7. When collecting personal data, the following information must also be provided: name and address of the respective LUXOFT entity describing that this entity is the data controller, name and address of any representative of the data controller and any other necessary information in order for the data subject to safeguard his/her interests.

8. In Denmark, when an entity collects personal data, it must inform the data subject if it is likely to disclose the data outside Denmark and specify the countries to which it will be disclosed (if the transfer is based on the data subject's consent only). If the transfer is based on SCCs, the controller must inform that it has taken steps to ensure that there is adequate protection for personal data in these circumstances.

9. The requirement to notify the data subject does not apply if the information is already known to the data subject. If the personal data is not provided by the data subject, the requirement to notify the data subject does not apply if notification is impossible or disproportionately difficult.

10. There is no mandatory obligation to notify the DPA. However, it is in some cases considered as good data processing practice to notify the data subject.

11. The conditions set out in section 4.6 are consistent with the PDA in relation to disclosure of personal data outside the EEA. Before an entity discloses personal information about an individual to an recipient established outside the EEA, including an associated or group entity, the entity must either make sure that the recipient ensures an adequate level of protection of personal data or expressly inform the individual that if he or she consents to the disclosure of information the entity will not need to ensure an adequate level of protection of personal data, and after being so informed the individual consents to the disclosure. The entering into EU Commission Standard Contractual Clauses ("**SCCs**") will provide an adequate level of protection of personal data. Please note that the Danish DPA considers even the smallest changes of the SCCs (e.g. changing commas and full stops) as "changes" which makes the SCCs "ad-hoc-contracts", which need authorization prior to the transfer commences. Further, the Danish DPA does not accept multi-signed SCCs. An individual SCC between each exporter and each importer should be made.

12. Processing of personal data is allowed when the processing is necessary in order to fulfil the employment contract between LUXOFT and the data subject. Processing of personal data in the workplace with consent as legal ground shall be limited to situations where the employee is provided with a de facto choice of whether he/she should accept the processing or not and where the employee at a later stage may withdraw his/her consent without facing any negative consequences.

13. Criminal records are considered semi-sensitive information. See note 6. In addition, while not prohibited, requesting criminal offence data can result in the risk of allegations of discrimination, if it is not relevant to the position.

14. If LUXOFT GROUP wishes to keep the data for future recruitment needs, the candidate must be informed accordingly and give his/her consent. Otherwise the data must be deleted as soon as possible and no later than 6 months after the refusal.

15. Pursuant to the PDA, monitoring of employees requires consent from the employee or a necessary operational reason. Further, the purposes of the monitoring should be assessed, and the employer should notify the employees of the monitoring prior to the monitoring. If the employees are employed under collective agreements, certain requirements regarding notification to the employees and the works council (if such council is in fact formed) may likely apply. For instance, the employer is obligated to inform and consult with the works council about the monitoring. This obligation has an informative purpose only. Further, a 6 weeks' prior notice before launching the monitoring should be observed. An individual employee cannot give binding consent to monitoring, if the employee is employed under a collective agreement. Please note that it is prohibited to read any private e-mails, documents or folders.

7. FRANCE

1. Under French Data Protection Law ("French DP Law"), purposes for processing personal data must also be determined, specific and legitimate.

2. Under French DP law, personal data which is processed must be adequate, relevant and non-excessive in relation to the purposes for which it is processed.

3. In addition to the right of access and correction, under French DP law, individuals benefit from the right of deletion and objection to the processing of their personal data upon legitimate grounds, as well as the right to give instructions as to the fate of the data subject's data after his/her death.

4. Under French DP law, any automated processing must be notified to the French Data Protection Authority ("the CNIL") unless an official Data Protection Officer has been appointed according to French law specific requirements. In specific cases, such as in case of a data transfer outside of the EU, an authorization from the CNIL is also required.

5. Under French DP law and according to the CNIL's guidance and case law, consent must be prior, explicit and specific (i.e. no consent is valid if given for several different purposes for instance). The consent must also be informed and freely given (i.e. no consent can be considered valid if the individual cannot refuse).

6. Under French DP law, the use of personal data for a purpose which was not notified to the CNIL is unlawful.

7. Under French DP law, additional data (not expressly designated as sensitive by the French DP Act) is also subject to specific requirements i.e. criminal offences and convictions, Social Security Number, biometric data and genetic dataa principle, the processing of sensitive data on employees is prohibited under French DP law. It may only be processed by the employer when specifically authorized by law.

8. Under French DP law, data subjects must also be informed about the retention periods of their personal data or, if this is not possible, the criteria used to determine this period.

9. Under French DP law, transfers of personal data outside the EU are subject to specific information requirements and individuals must be informed of the following elements: i) the list of countries outside of the EU where the data is transferred, ii) the categories of personal data that is transferred, iii) the purposes of the transfer, iv) the categories of recipients of the data transferred, and v) the safeguards implemented for ensuring an adequate level of protection to the transfer (i.e. EU standard contractual clauses, Privacy Shield for the US, Binding Corporate Rules).

10. When personal data is collected through a form/questionnaire, the following information must be mentioned directly on the form: i) the identity of the data controller and of its representative, if any; ii) the purposes for which personal data is processed; iii) whether providing data is mandatory or optional and the possible consequences of the absence of a reply; and, iv) the data subject's rights of access, correction, deletion and objection to the processing of personal data upon legitimate grounds as well as the right to give instructions as to the fate of the data subject's data after his/her death.

11. Such exemption does not apply under French DP law.

12. Direct marketing communication to individuals via electronic means (i.e. emails, text messages) is subject to obtaining the individuals' consent for instance via a box to be ticked ("opt-in"). This does not apply to direct marketing communication between professionals, who must be offered a mean to object to the sending of such communication in each message ("opt-out").
    Direct marketing communication to individuals over the phone or by post requires to provide a mean to object to such communication ("opt-out"). In any case, all the mandatory information notice required by French DP law must be provided to the individual.

13. Failure to comply with French DP law may lead to both administrative sanctions (up to 3,000,000 €) and criminal sanctions (up to 5 years of imprisonment and a fine up to 300,000 €).
14. cannot be a valid ground for processing employees' data since, according to French Labour law and the CNIL's guidance, consent from an employee is not considered as freely givena principle, the collection of personal data on criminal offences and conviction is prohibited under French DP law.

15. Under French DP law and Labour law, prior information and consultation of the Works Councils ("Comité d'entreprise" and "Comité d'hygiène, de sécurité et des conditions de travail") is mandatory in the following

circumstances: i) the implementation of new technologies that may have an impact on the working conditions, and ii) the implementation of technologies which allow to monitor the employees (for instance: setting up of a CCTV system, recording of the phone conversations, using geo-tracking devices).

16. If LUXOFT wishes to keep the CVs of unsuccessful applicants for future use, the relevant applicants must be informed of such processing, and should also give his/her consent according to the CNIL's guidance.

17. In accordance with the CNIL's guidance, the collection of some information on job applicants is forbidden in France:

a. Date of entry into France, date of naturalization, modalities for the grant of French nationality and original nationality;
b. Social security number;
c. Details about military situation;
d. Former address;
e. Information about applicants' family (i.e. their name, nationality, job and employer);
f. Health status, size, weight, eyesight;
g. Housing conditions (owner or tenant);
h. Associative life;
i. Banking information, loans contracted, defaults on payments.

18. French DP and Labour law, several requirements apply to the monitoring of employees including:

i) Prior information and consultation of Works Councils ("Comité d'entreprise" and "Comité d'hygiène, de sécurité et des conditions de travail"), no approval required;

ii) Prior notification to the CNIL of the data processing relating to employee monitoring, except if a Data Protection Officer (DPO) has been appointed (in which case, the data processing must be mentioned in the DPO's register). In addition, if personal data is transferred outside of the EU, an authorization from the CNIL would be required;

Prior notice to employees which should specify in particular the scope of the monitoring, its purposes, the recipients of the data collected and the data retention period.accordance with French Labour Law, the notice/policy on monitoring rules should be annexed to the Internal Ruling ("Règlement intérieur") to allow disciplinary sanctions against employees if they do not apply the rules on the use of IT systems.

19. Under French law, emails received or sent by employees using their professional email address/account are presumed to be of a professional nature and may be thus accessed by the employer any time, without prior notice, including in the absence of the employee.

The employer cannot access the employees' private emails (i.e. either because it is titled "private" or "personal" or because after the employer starts reading it appears that the content is private – then the employer should stop reading) without the consent or the presence of the employee. In order to be of the safe side, it is advisable to obtain a court order to be allowed to open a private email.

8. GERMANY

1. If Luxoft Germany has a works council, the implementation of the privacy policy could be subject to co-determination rights.

2. It is usually not permitted to collect criminal conviction data unless the job specifically requires it (e.g. financial crimes for a cashier).

3. Access to e-mails of employees marked as private / personal is generally not permissible. Emails which are clearly marked as personal or private may not be read or further processed. Personal use of LUXOFT GROUP's email systems is not permitted for German employees. Please be aware that the interception of emails which are not archived may constitute a criminal offence.

4. Before CCTV is introduced into areas which are not freely accessible to the public (including the car park and the reception area) you must seek guidance from the Data Protection Officer. German law on CCTV on company premises is subject to very strict rules and only permitted in very limited circumstances. Any kind of illegal monitoring is very sensitive in Germany and can lead to severe fines and a negative public image.

9. INDIA

1. According to the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal data or Information Rules,2011) (hereinafter referred to as the "Privacy Rules"), Sensitive Personal Data or Information also includes passwords; financial information such as bank account or credit card or debit card details and/or other payment instrument details; information regarding physical, physiological and mental health conditions; medical records and history; biometric information; any detail relating to the foregoing as provided to the LUXOFT GROUP for providing any service(s); and any of the aforementioned information received by LUXOFT GROUP for processing or storage, whether under a lawful contract or otherwise:

The Privacy Rules further provide that any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these rules.

In India, there is no legal requirement to appoint a Data Protection Officer. However, LUXOFT GROUP shall address any discrepancies and grievances of the data subject, with respect to processing of information, in a time bound manner and shall designate a Grievance Officer for this purpose and publish his/her name and contact details on its website. The Grievance Officer shall redress the grievances of the data subject expeditiously and shall ensure that it is done within one (1) month from the date of receipt of grievance;

2. The Privacy Rules mandate that Sensitive Personal Data or Information shall not be collected, unless the said information is to be collected for a lawful purpose which is connected with a function or activity of the collector; and the collection of such information is necessary for that purpose. The information so collected may be used only for the purpose for which it has been collected. The Privacy Rules further mandate that the LUXOFT GROUP shall put in place a privacy policy (containing the prescribed particulars) for handling of or dealing in personal information and sensitive personal information, shall ensure that it is available for view by the data subjects and shall publish the same on its website.

3. The Privacy Rules mandate that the LUXOFT GROUP shall, prior to the collection of information including Sensitive Personal Data or Information, provide an option to the data subject not to provide the data or information sought. Should the data subject choose to provide Sensitive Personal Information, that the LUXOFT GROUP shall, prior to collection of Sensitive Personal Data or Information, obtain from the data subject, consent in writing by way of letter, fax or e-mail regarding the purpose for its use. The data subject shall, at any time have an option to withdraw his/her consent. Such withdrawal of the consent shall be sent in writing to the concerned department in the LUXOFT GROUP. In the case of the data subject not providing or later withdrawing his/her consent, the LUXOFT GROUP shall have the option not to provide goods or services for which the said information was sought. ***[Note: The Privacy Rules allow the data subject the option to refuse to provide information or to withdraw consent once given. In light of the same the LUXOFT GROUP should determine the course of action to be adoped in the event the data subject refuses to provide data or later withdraws consent.]***

4. The Privacy Rules mandate that while collecting information directly from the data subject, the LUXOFT GROUP shall take such steps as are, in the circumstances, reasonable to ensure that the data subject is aware of— (a) the fact that the information is being collected; (b) the purpose for which the information is being collected; (c) the intended recipients of the information; and (d) the name and address of — (i) the agency that is collecting the information; and (ii) the agency that will retain the information.

5. The Privacy Rules mandate that the LUXOFT GROUP shall not publish Sensitive Personal Data or Information that it has collected and further mandates that any disclosure of Sensitive Personal Data or Information collected from a person under a lawful contract, to a third – party, shall require the prior permission of the data subject, unless the disclosure thereof has been agreed to by the data subject, in the said contract or where the disclosure is necessary for compliance of a legal obligation. Sensitive Personal Data or Information can also be disclosed to mandated government agencies without prior consent of the data subject or to a third party by an order under the law for the time being in force. The Privacy Rules specify that any third party receiving such Sensitive Personal Data or Information shall not disclose it further.

6. The Privacy Rules also mandate that the LUXOFT GROUP may transfer Sensitive Personal Data or Information only if it is necessary for the performance of the lawful contract between the LUXOFT GROUP and the data subject or where such person has consented to the transfer of such information.

7. The Privacy Rules mandate that the LUXOFT GROUP shall comply with reasonable security practices and procedures with respect to Personal Data, including Sensitive Personal Data as follows:

(i) A comprehensive documented information security programme and information security policy that contains managerial, technical, operational and physical security control measures that are commensurate with the data or sensitive personal data being protected with the business is to be implemented;

(ii) In the event of an information security breach, the LUXOFT GROUP shall be required to demonstrate, as and when called upon to do so by the agency mandated under the law that security control measures have been duly executed as per the documented information security programme and information security policy;

(iii) Security practices and standards such as the international standard IS/ISO/IEC 27001 on “Information Technology -Security Techniques -Information Security Management System or other codes of best practices duly approved and notified by the central government of India shall be implemented;

(iv) Such standards or codes of best practices are to be certified or audited on a regular basis by entities or an independent auditor, duly approved by the central government. Such audit shall be carried out at least once a year or as and when the LUXOFT GROUP undertakes a significant upgradation of its processes and computer resources.

8. LUXEMBOURG

1. The Luxembourg Act of 2 August 2002 on the protection of individuals with regard to the processing of personal data (the "Data Protection Act") does not restrict the concept of 'personal data' to *living* individuals. Any information of any type regardless of the type of medium relating to an identified or identifiable natural person qualifies as personal data, regardless of whether this natural person is alive or deceased.

2. Pursuant to the Data Protection Act, there is no requirement of notification to the Luxembourg data protection authority (the National Commission for Data Protection) if:

   - The data controller has designated a data protection officer, unless in case of processing for surveillance purposes. This exemption only applies if such data protection officer has been approved by the Luxembourg data protection authority;

   - The processing of data – with the exclusion of sensitive data – takes place for HR management purposes, unless this data is used to assess the data subject.

3. The Data Protection Act also indicates genetic data as sensitive personal data. Moreover, data on offences, criminal convictions or security measures may only be processed in execution of a legal provision.

4. Under Luxembourg law, at least the information regarding the LUXOFT GROUP entity and the purposes for which the LUXOFT GROUP processes the personal data should be provided.

5. Please note that in certain instances, such as surveillance at the workplace, consent of the employee cannot constitute a legitimate condition for data processing by the employer.

6. The Luxembourg Criminal Records Act of 29 March 2013 explicitly allows the employer to request an employee or job applicant to produce an extract of his criminal record for the purposes of management and recruitment of staff. This extract, as well as the data contained therein, may not be kept for more than 2 years.

7. Pursuant to Article L. 261-1 of the the Luxembourg Employment Code, the employee must be notified that the monitoring will be carried out. Must also be notified: the joint company committee, the staff delegation or the Labour and Mines Inspectorate for employees falling within the scope of the legislation on private contracts and the employee representative bodies for the persons with a statutory employment status.

8. Please note that communications clearly marked as personal may not be read, even in exceptional circumstances where a problem relating to an employee’s excessive or unauthorised use is suspected.

9. The use of CCTV in the workplace is subject to prior authorisation by the Luxembourg data protection authority, unless only non-employees are monitored without recording. In the latter case, a notification with the Luxembourg data protection authority suffices.

9. MALAYSIA

1. In Malaysia, the Personal Data Protection Act 2010 ("PDPA") defines "personal data" as any information in respect of commercial transactions, which (i) is being processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose; (ii) is recorded with the intention that it should be wholly or partly processed by means of such equipment; or (iii) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, that relates directly or indirectly to a data subject, who is identified or identifiable from that information or from that and other information in the possession of a data user, including any sensitive personal data and expression of opinion about the data subject. It does not include any information that is processed for the purpose of a credit reporting business carried on by a credit reporting agency under the Credit Reporting Agencies Act 2010. The scope of protection is limited to personal data of living individuals and it does not include information about a dead individual nor does it cover other persons such as companies or businesses.

2. LUXOFT GROUP may not transfer the personal information of an individual to places outside Malaysia unless to such place as specified by the Minister, upon recommendation of the Commissioner, by notification published in the Gazette in which case the Minister may specify any place outside Malaysia if:

   a. there is in that place in force any law which is substantially similar to the PDPA, or that serves the same purposes as the PDPA; or
   b. that place ensures an adequate level of protection in relation to the processing of personal data which is at least equivalent to the level of protection afforded by the PDPA.

   LUXOFT GROUP may transfer any personal data to a place outside Malaysia if:

   a. the individual consents to the transfer;
   b. the transfer is necessary for the performance of a contract between the individual and LUXOFT GROUP;
   c. the transfer is necessary for the conclusion or performance of a contract between LUXOFT GROUP and a third party which is entered into at the request of the individual or is in the interests of the individual;
   d. the transfer is for the purpose of any legal proceedings or for the purpose of obtaining legal advice or for establishing, exercising or defending legal rights;
   e. LUXOFT GROUP has reasonable grounds for believing that in all circumstances of the case (i) the transfer is for the avoidance or mitigation of adverse action against the individual; (ii) it is not practicable to obtain the consent in writing of the individual to that transfer; and (iii) if it was practicable to obtain such consent, the individual would have given his consent;
   f. LUXOFT GROUP has taken all reasonable precautions and exercised all due diligence to ensure that the personal data will – in that place – not be processed in any manner which, if that place was Malaysia, would be a contravention of the PDPA;
   g. the transfer is necessary to protect the vital interests of the individual; or
   h. the transfer is necessary as being in the public interest in circumstances as determined by the Minister.

3. In Malaysia, there is no requirement to appoint a Data Protection Officer. However, a data subject must be given access to his personal data and has the right to correct it if it is inaccurate, incomplete, misleading or out-of-date. The data subject must make the request in writing and pay the prescribed fee to have a copy of his personal data. LUXOFT GROUP must comply with the request not later than 21 days or must inform why it is unable to comply within that period. LUXOFT GROUP must still comply no later than another 14 days after expiration of the first 21 days unless the following exceptions apply:

   a. The data exporter may refuse to comply with a data access request within the prescribed 21 days period or a further 14 days period if:
      - the data exporter is not supplied with such information as he may reasonably require in order to satisfy himself as to the identity of the requestor;
      - the data exporter is not supplied with such information as he may reasonably require, where the requestor claims to be a relevant person, in order to satisfy himself as to the identity of the data subject in relation to whom the requestor claims to be the relevant person, and that the requestor is the relevant person in relation to the data subject;
      - the data exporter is not supplied with such information as he may reasonably require to locate the personal data;
      - the burden or expense of providing access is disproportionate to the risks to the data subject's privacy in relation to the personal data;
      - the data exporter cannot comply with the data access request without disclosing personal data relating to another individual who can be identified from that information unless that other

individual has consented to the disclosure of the information to the requestor or it is reasonable in all circumstances to comply with the data access request without such consent;

- any other data user controls the processing of the personal data in such a way as to prohibit the data exporter from complying, whether wholly or partly, with the data access request. This, however, shall not operate so as to excuse the data exporter from complying with the data access request to any extent that the data exporter can comply with the request without contravening the prohibition;
- providing access would constitute a violation of an order of a court;
- providing access would disclose confidential commercial information; or
- such access to personal data is regulated by another law.

b. Separately, a data correction request need not be complied with if:

- the data exporter is not supplied with such information as he may reasonably require in order to satisfy himself as to the identity of the requestor;
- the data exporter is not supplied with such information as he may reasonably require, where the requestor claims to be a relevant person, in order to satisfy himself as to the identity of the data subject in relation to whom the requestor claims to be the relevant person, and that the requestor is the relevant person in relation to the data subject;
- the data exporter is not supplied with such information as he may reasonably require to ascertain in what way the personal data is inaccurate, incomplete, misleading or not up-to-date;
- the data exporter is not satisfied that the personal data is inaccurate, incomplete, misleading or not up-to-date;
- the data exporter is not satisfied that the correction is accurate, complete, not misleading or up-to-date; or
- any other data user controls the processing of the personal data in such a way as to prohibit the data exporter from complying, whether wholly or partly, with the data correction request. This, however, shall not operate so as to excuse the data exporter from complying with the data correction request to any extent that the data exporter can comply with the request without contravening the prohibition.

4. The PDPA is silent on whether an express or implied consent is required. The Personal Data Protection Regulations 2013 (“Regulations”), which stipulates that consent must be “recorded” and “maintained”, suggests that express consent is required. However recent proposal papers indicate that implied consent may be sufficient provided the individual has been made fully aware of the purposes of the processing of his personal data and as long as the data user is able to demonstrate that consent has been given by the individual.

5. Sensitive personal data also includes information as to the commission or alleged commission of any offence or any other personal data declared by the Minister to be sensitive personal data.

6. It is also necessary to provide any information available to LUXOFT GROUP about the source of that personal data, how to contact LUXOFT GROUP with any inquiries or complaints in respect of the personal data and the choices and means which LUXOFT GROUP offers the individuals for limiting the processing of personal data, including personal data relating to other persons who may be identified from that personal data. Information provided must be in national and English languages.

7. According to the PDPA, this information should arguably be provided as there are no specific exceptions to the notice and choice principle which requires notice and disclosure for business contact information. However, in practice this is usually not observed. Notwithstanding the aforesaid, such business contact information may arguably be regarded as falling outside the definition of “personal data”. If the commercial transaction is between LUXOFT GROUP and a company, the personal data of representatives of the said company is arguably not “personal data” within the meaning of the PDPA as it is not in respect of commercial transactions that relate directly or indirectly to the representative (individual) of the said company. Therefore, such personal data might not be subject to the PDPA.

8. It is recommended that LUXOFT GROUP obtains consent from the employees when collecting normal personal data. However, the consent requirement is exempted for the performance of a contract to which the employee is a party. To qualify for exemption, LUXOFT GROUP must evaluate and determine what information is absolutely necessary for the discharge of the duties and obligations of both LUXOFT GROUP and the employee to avoid excessive data collection.

9. It is recommended that consent must be obtained from the unsuccessful applicants if LUXOFT GROUP needs to retain such personal data for other purposes including future use.

10. LUXOFT GROUP is not allowed to share data with third parties unless the consent of the employee is obtained.

11. Consent of the employees is required before sending direct marketing material to them. In addition, the employee must be given a right to refuse such use of their personal data at the time the data is collected using a free “opt-out” possibility.

12. LUXOFT GROUP is not allowed to disclose information about an employee for any purpose other than employment or to any third party other than the categories of people who will receive the data, of which the employee is fully aware and to which the employee has given consent. Nevertheless, personal data of the employee may be disclosed for any other purpose only under the following circumstances:

    a. the employee has given his consent to the disclosure;
    b. the disclosure is necessary for the purpose of preventing or detecting a crime, or for the purpose of investigations;
    c. the disclosure was required or authorized by or under any law or by the order of a court;
    d. LUXOFT GROUP acted in the reasonable belief that it had a legal right to disclose the personal data to the other person;
    e. LUXOFT GROUP acted in the reasonable belief that it the employee had given its consent if the employee had known of the disclosing of the personal data and the circumstances of such disclosure; or
    f. the disclosure was justified as being in the public interest in the circumstances as determined by the Minister.

13. In Malaysia, LUXOFT GROUP can only install CCTV at workplace for the purpose of crime detection and prevention. It cannot be used for other purposes such as staff monitoring. Upon installation of CCTV, LUXOFT GROUP shall display a notice that is visible to visitors and place it at the entrance to the CCTV surveillance zone, informing them of the CCTV operation and the purposes for installation.

14. A third party service provider (“data processor”) who processes information on behalf of LUXOFT GROUP shall process such information only with the knowledge and authorisation of LUXOFT GROUP. LUXOFT GROUP shall, for the purpose of protecting the personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction, ensure that the data processor:

    a. provides sufficient guarantees in respect of the technical and organizational security measures governing the processing to be carried out; and
    b. takes reasonable steps to ensure compliance with those measures.

15. There is no statutory retention period for the storage of CCTV images. It is recommended that the retention period should reflect the purpose of recording by LUXOFT GROUP. Images may be kept longer if needed for the purpose of investigation by law enforcement agencies. However, they must be deleted if there is no reason to keep them.

16. An individual’s image from the CCTV intended to be used by LUXOFT GROUP for the purposes agreed to by the individual must be clear, accurate and not misleading. LUXOFT GROUP may consider using suitable cameras depending on location and field of view to ensure images captured are of high quality, clear and precise. LUXOFT GROUP also has to ensure the same responsibility extends to any external processor LUXOFT GROUP intends to use for processing the CCTV footage.

17. Individuals have the right to view their own image captured upon their request. However, procedures for access along with necessary details from the individual should be provided explicitly by LUXOFT GROUP to confirm his/ her request for access to his/ her images only.

10. MEXICO

1. In Mexico a data subject also has the right to request that his personal data is deleted or cancelled (ARCO rights: the right to access, rectify or correct his data, cancel and oppose to certain types of processing). Cancellation of the personal data does not proceed automatically, therefore the specific situation has to be consulted with the Data Protection Officer to determine the course of action.

2. Under the Federal Law on the Protection of Personal Data held by Private Parties, there is no need for filings with the data protection authority.

3. The individual or data subject also has the right to request that his personal data is deleted or cancelled.

4. Even where consent is not required, the data subject must always be informed of the characteristics of processing of his data.

5. Use of data for a new purpose must always be informed to the data subject and in certain cases consent must also be requested.

6. Personal use of LUXOFT GROUP's email systems may be permitted as the client considers. However, if permitted, employees must be informed of the monitoring that may be carried out so that there is no expectation of privacy. Employees must be clear that email and other communications technologies are considered work tools subject to monitoring by the employer. The Data Protection Authority has not yet issued a resolution in this regard, where it clarifies if company email may or may not be accessed even when marked as personal. Please be aware that the interception of emails may constitute a criminal offence.

11. The Netherlands

1. Please note that in the Netherlands, photos and videos are also regarded as special personal data, and of a sensitive nature as they convey racial qualities of persons on the images. Because of this, the use of such personal data (i.e.. with CCTV and photo ID's on intranet) is subject to stricter rules.

2. If Luxoft Netherlands has a works council, the implementation of the privacy policy and any subsequent introduction of systems aimed at or capable of being used for monitoring the presence/absence, behaviour/conduct or performance of its personnel could be subject to co-determination rights, which may include prior consent from the works council.

3. Please note that due to the dependent relationship between employee and employer, consent given by employees is often not considered free.

4. The Dutch Data Protection Authority (**DPA**) states that employers are not allowed to access emails which are clearly marked as private. There might be some room for nuance in that statement, but it is advised to consult with a specialist or external counsel should Luxoft Netherlands wish to access private emails.

5. It is required to sufficiently address the matter of personal data breaches in a Data Processor Agreement, or any contractual clauses serving similar goals. It is also advised to include a section on Data Breaches in the specific Annexes for Sales, IT and Facilities to increase awareness.

12. POLAND

1. If you collect personal data about individuals, you must provide also the following information: name of LUXFORT entity indication that it is a data controller, its registered office and address.

2. According to Polish law this information should be provided. However, in practice this is usually not observed and at the time being the Polish DPA does not enforce this requirement.

3. In Poland it would be recommended to obtain a consent for processing data of the job applicants

4. In Poland, you cannot collect details about illnesses, only absence information (except tuberculosis).

5. Do not ask for details of criminal offences unless this is necessary for the position and specific regulations allow for it.

6. You must explain to the unsuccessful applicants if you want to keep CVs on file for future use and CVs should only be retained if the applicant gives explicit consent.

7. Under Polish law the employer cannot read emails if it knows that it concerns private matters. Emails which are clearly marked as personal should not be read even in the exceptional circumstances where a problem relating to an employee's excessive or unauthorised use is suspected. Personal use of LUXOFT GROUP's email systems for Polish employees is not permitted.

8. The list of processed categories of personal data should be exhaustive. The purpose(s) of the processing should also me mentioned. The data processing agreement should be in writing (hard copy document with handwritten signatures).

9. For Poland the following list of mandatory security measures should be implemented.

Poland: Data Protection Security Requirements

1. General obligatory security measures

a) The controller/processor is obliged to appoint a controller/processor of information security (in Polish: *administrator bezpieczeństwa informacji*).
b) Only persons who were granted authorization by the controller/processor should be allowed to carry out data processing.
c) The controller/processor should keep a register of the persons authorised to carry out data processing , which should contain the following:
   i) full name of the authorised person,
   ii) date of granting and expiration, as well as the scope of authorisation to access personal data,
   iii) identifier, in cases where data are processed in an IT system,
d) The persons authorised to carry out the data processing shall be obliged to keep these personal data and the ways of their protection confidential.

2. Compulsory documentation

A data controller/processor is obliged to keep and implement written documentation regarding data security principles.

The documentation should consist of: (1) the Security Policy and (2) instruction for using the data processing IT system (the "**IT Instruction**").

The Security Policy
The Security Policy should include in particular:
a) a list of buildings, premises or their parts comprising the area where the personal data are processed ('area were data are processed');
b) a list of data filing systems with an indication of software used for data processing. According to Polish law, a data filing system is a set of personal data that have a structure, is centralised or decentralised, and where data are available on the basis of at least one criterion);
c) a description of the structure of the data filing systems and indication of the content of particular information fields and connections between them;
d) method of transferring data between particular systems;
e) a definition of technical and organisational measures necessary to ensure confidentiality, integrity and accountability of the data being processed.

IT Instructions

The IT Instructions should consist of, in particular:

a) procedures for granting authorisation to process data by users (e.g. employees) and registration of these authorisations in the IT system, as well as indication of the person responsible for granting authorisations (e.g. *privacy officer/IT manager*);
b) methods and means of users' authorisation and procedures connected with the management and use of those methods and means;
c) procedures of beginning, suspending and terminating work by users of the IT system;
d) procedures of making backups of the data filing systems and programs and software tools used for the data processing (together with the location of backup copies);
e) method, place and period of storage of: (a) data carriers, and (b) backups referred to in point d);
f) method of securing the IT system against software serving for gaining unauthorised access to IT systems;
g) how the requirement is met that the IT system should allow for recoding of information on recipients to whom the data were disclosed and the date and scope of this disclosure;
h) procedures for inspecting and maintaining IT systems and data carriers used for personal data processing.

3. Specific obligatory security measures

Most controller/processors in Poland are obliged to apply a high level of security. The high level of security applies when the controller/processor uses an IT system that is connected to the Internet (at least by one device).

The following are minimum requirements in order to apply the high level of security:

a) Buildings, premises or their parts comprising the area where data are processed should be secured against access of unauthorised persons during the absence in this area of the persons authorised to process personal data.
b) Any unauthorised person may stay inside the area where the personal data are processed only upon the controller/processor's consent or in the presence of a person authorised to process personal data.
c) The mechanisms of access control should be applied in the IT system used for personal data processing.
d) A separate identifier should be registered for each IT system user.
e) Access to data should be available only after entering the identifier and the user's authentication.
f) The IT system used for personal data processing should be secured in particular against:
g) software used for gaining unauthorised access to the IT system;
h) loss of data which may be caused by any power supply failure or line interference.
i) The identifier of a user who has lost authorisation to personal data processing should not be granted to another person.
j) In the case where the password is used for user's authentication, the passwords should be changed at least once a month. In the case where the password is used for user authentication, the password should consist of at least eight characters, including small and capital letters, numbers and special characters.
k) Personal data being processed within the IT system should be secured by making back-ups of the data filing systems and using data processing software.
l) Back-ups should:
m) be stored in the premises ensuring security against any unauthorised takeover, change, damage or destruction;
n) be deleted as soon as their usefulness ceases.
o) A person using a laptop containing personal data should be obliged to take special precautions while having the laptop transported, stored or used outside the area where data are processed, including cryptographic protection measures.
p) Devices, discs and other electronic information media containing personal data intended to:
    i) liquidation – should be devoid of those data, and in cases when it is impossible, the records should be damaged,
    ii) be turned over to any other party unauthorised to process personal data – should be devoid of the personal data,
    iii) be repaired – should be devoid of those data, thereby to make them not retrievable or should be repaired under supervision of a person who has been authorised.
q) The controller/processor should supervise the security measures to be implemented within the IT system.
r) Any devices and information media containing sensitive data being transferred outside the area where the personal data are processed should be secured in such a way to ensure confidentiality and integrity of these data – (according to the DPA, devices should be encrypted) (the IT instruction should cover the method of the application of this security measures).
s) The IT system used for personal data processing should be secured against any dangers originating from the Internet by the implementation of physical and logical security measures protecting against any unauthorised access (according to the DPA, personal data transferred via Internet should be encrypted).
t) In cases where the logical security measures referred to in point 15 are applied, these measures should cover:
u) control of data flow between the IT system of the controller/processor and the Internet;
v) control of actions initiating from the Internet and the IT system of controller/processor.
w) The controller/processor should apply cryptographic protection measures for the data used for authentication which are being transferred within the Internet

x) IT systems used by the controller/processor to process personal data must also provide functionality that allows keeping a record of:
   a. the date when the personal data have been registered for the first time in the IT system,
   b. an identifier of a user who registers the personal data in the IT system,
   c. sources of personal data, if personal data have not been obtained from the data subject,
   d. information on recipients ((i) to whom personal data have been disclosed and (ii) the date thereof and (iii) the scope of this disclosure),
   e. any objection of the data subject to process their data.

This should be an automatic process. IT systems should save the data mentioned above after an authorised user enters data subjects' personal data to the IT system. Implementation and the whole process must be documented.

13. ROMANIA

1. Details about sickness can be recorded only if needed for compliance with the specific obligations of LUXOFT GROUP in labour field (e.g., for documenting the employees' absence).

2. Details of criminal offences should not be requested, unless such is legally requested for holding the respective position.

3. You must inform the unsuccessful applicants that you want to keep CVs on file for future use and CVs should only be retained if the applicants give their explicit consent on such.

4. Monitoring of employees' correspondence on a continuous basis (active monitoring) is not allowed. Likewise, monitoring/ processing of employees' e-mails clearly marked as "Private" or monitoring of employees' discussions by telephone or by way of other electronic communications means is strictly forbidden and may qualify as criminal offence.

5. The existence/ using of the CCTV needs to be pointed out by using a pictogram of an appropriate size and placed at a reasonable distance from the place where the CCTV cameras are installed. Generally, the use of CCTV within the area of the offices is strictly forbidden, save for the case where made based on the prior approval of the Romanian supervisory authority. Also, the use of hidden CCTV cameras is not allowed, unless in the limited cases set forth by the law. In no case may CCTV be used in places which, by their nature, impose the preservation of intimacy (e.g. toilettes).

14. RUSSIA

1. In Russia express consent of an employee in writing is necessary if the data is transferred to any third party and/or sensitive data (like religious beliefs) is collected and processed.

2. Processing information on criminal offences is prohibited except when the disclosure of this data is required by law for the purposes of employment.

3. In Russia an employee shall be aware about and give his/her written consent for any data transfers including those within or outside Russia.

4. The employer is prohibited from making decisions relating to employees based solely on data received automatically or electronically.

5. Sensitive information may be collected and processed only upon a written consent of the candidate; it is impossible to collect this information through the website.

6. The unsuccessful candidates should give their consent on the processing of personal data from their CV. Such consent can be granted in any form which can demonstrate that the consent is specified, well-informed and in full awareness. We recommend written form.

7. Background checks with third parties are allowed only upon written consent of the employee.

8. Written consent of a candidate shall be necessary for data transfers to the countries not providing an adequate protection for the personal data (i.e. having no unified law on a data protection and enforcement authorities).

9. In general monitoring of employee's e-mails and personal electronic activities may be interpreted as interference into private life or violation of secrecy of correspondence. Both constitute a criminal offense. Thus monitoring may not take place without express consent of an employee in writing.

15. SINGAPORE

1. "Personal data" under the Singapore Personal Data Protection Act 2012 ("PDPA") is defined as data, whether true or not, about an individual who can be identified from that data or from that data and other information to which an organisation has or is likely to have access. The data protection obligations under the PDPA do not apply to business contact information and the PDPA does not apply to personal data about deceased individuals except in relation to disclosure and protection of personal data of an individual who has been dead for 10 years or less. No consent is required for the collection, use or disclosure of personal data that is publicly available.

2. Generally, staff may only collect, use, disclose or otherwise process personal data for particular purposes where LUXOFT GROUP has first obtained consent for the collection, use or disclosure of the personal data for those purposes, unless exempted under the PDPA.

3. Under the PDPA, an organisation must not transfer any personal data to a country or territory outside Singapore unless it provides a standard of protection to the transferred personal data that is comparable to the protection under the PDPA.

4. LUXOFT GROUP has been provided with PDPA-compliant data transfer agreements to regulate the transfers of personal data out of Singapore.

5. Staff should seek the input of the Data Protection Officer if you are not sure whether a data transfer agreement is in place to facilitate the transfer of personal data out of Singapore to a third party or country.

6. New Uses: Under the PDPA, use of personal data for a new purpose will require fresh consent. Staff must therefore consult the Data Protection Officer if they wish to use personal data for a new purpose.

7. Access: Under the Singapore Personal Data Protection Regulations 2014, organisations must provide a written response to access and correction requests within 30 days. If an organisation cannot respond within 30 days, it must inform the individual in writing of when it expects to be able to respond to the request. Requests should therefore be forwarded promptly to the relevant persons responsible so that the organisation can comply with the statutory timeline.

8. The PDPA only imposes the retention and protection obligations on data processors, known as “data intermediaries” in Singapore. However additional obligations may be contractually imposed, as has been done in Supplementary Document 4. Supplementary Document 4 may be used to facilitate disclosures to third-party data intermediaries in Singapore with the appropriate changes (e.g. change references of the Directive to the Singapore Personal Data Protection Act, change references to the EEA to Singapore, etc.).

9. Transparency: There is no consent exception for visitors under the PDPA. We recommend that visitors are provided with purpose notification language prior to the Company collecting, using or disclosing their personal data when they visit the premises to obtain consent for stated purposes.

10. Retention: Under the PDPA, Luxoft must cease to retain personal data (i) as soon as it is reasonable to assume that the purpose for which that personal data was collected is no longer being served by retention of the personal data; and retention is no longer necessary for (ii) legal or (iii) business purposes. Therefore the 3 year period must be justifiable on one of the above three grounds.

16. SOUTH AFRICA

1. The Protection of Personal Information Act, 4 of 2013 (the "Act") was signed into law in 2013. While certain provisions of the Act are in effect, the commencement date of the remaining provisions of the Act has not yet been proclaimed by the President. Where the data controller is domiciled in South Africa or processes personal information in South Africa (unless only to forward personal information through South Africa), the Act will be applicable.

2. "Personal Information" includes information relating to an identifiable, existing juristic/legal person.

3. LUXOFT GROUP may not transfer the personal information of an individual to a third party in a foreign country unless:
    a. the recipient is subject to a law, binding code of conduct or contract which:
        i. upholds principles for processing of information that are substantially similar to the information protection principles contained in the Act;
        ii. includes provisions, that are substantially similar to the provisions in the Act relating to the further transfer of personal information from the recipient to third parties who are in a foreign country;
    b. the individual consents to the transfer;
    c. the transfer is necessary for the performance of a contract between the individual and LUXOFT GROUP;
    d. the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between LUXOFT GROUP and a third party; or
    e. the transfer is for the benefit of the individual, and:
        i. it is not reasonably practicable to obtain the consent of the individual to that transfer; and
        ii. if it were reasonably practicable to obtain such consent the individual would be likely to give it.

4. This will not be necessary in South Africa as LUXOFT GROUP requires that its third party operators and its data importers comply with certain security measures in its contractual arrangements with these parties.

5. Where there are reasonable grounds to believe that the personal information of an individual has been accessed by an unauthorised person, LUXOFT GROUP must notify the South African information regulator and the individual (if the identity of the individual can be established).

6. The processing of information concerning personnel in the service of the LUXOFT GROUP must take place in accordance with the rules established in compliance with labour legislation.

7. Sensitive personal information may be processed if:
    a. the consent of the individual is obtained;
    b. necessary for the establishment, exercise or defence of a right or obligation in law;
    c. necessary to comply with an obligation of international public law;
    d. processing is for historical, statistical or research purposes to the extent that-

        iii. the purpose serves a public interest and the processing is necessary for the purpose concerned; or

        iv. it appears to be impossible or would involve a disproportionate effort to ask for consent, and sufficient guarantees are provided for to ensure that the processing does not adversely affect the individual privacy of the data subject to a disproportionate extent;
    e. information has deliberately been made public by the individual; or
    f. concerning an individual's race or ethnic origin only if essential to identify the individual for the purpose of processing or comply with laws and other measures designed to protect or advance persons, or categories of persons, disadvantaged by unfair discrimination.

8. The additional processing of information is restricted to only those instances where the purpose for the further processing is "compatible" with the original purpose for which the personal information was collected. Should the disclosure of the information not be for purposes of fulfilling a legal duty placed on the LUXOFT GROUP or compatible with the original purpose for which the information was collected, the consent of the individual will be required.

9. LUXOFT GROUP may intercept the communication of an employee if such employee has provided his/her prior written consent to such interception. This may be in the form of an internet usage or email policy which is incorporated into the employee's contract of employment with LUXOFT GROUP. Monitoring of IT Equipment and IT Network may be carried out without the consent of the employee in order to secure the effective operation of the system, establish the existence of certain facts or to detect unauthorised use of the system.

10. A third party processing personal information on behalf of LUXOFT GROUP must process such information only with the knowledge or authorisation of LUXOFT GROUP, and treat the personal information as confidential and must not disclose it, unless required by law or in the course of the proper performance of their duties. LUXOFT GROUP shall ensure that such third party establishes and maintains security measures to prevent the loss of, damage to or unauthorised destruction of personal information; and unlawful access to or processing of the personal information.

11. The Service Provider shall notify the Luxoft Entity immediately or as soon as reasonably practicable if any personal information has been or may reasonably believed to have been accessed or acquired by an unauthorised person or if a security breach has occurred.

12. Where a LUXOFT GROUP entity is processing personal information on behalf of a data controller (such as a customer), it must:

    a. process such information only with the knowledge or authorisation of the data controller; and
    b. treat personal information which comes to its knowledge as confidential and must not disclose it,

    unless required by law or in the course of the proper performance of its duties.

17. SWEDEN

15. Under the Swedish Personal Data Act ("**PDA**") a data subject has the right to request access and to request the controller to correct, block or erase such personal data that has not been processed in accordance with Swedish law.

16. Under the PDA, the legitimate interest of the controller must outweigh the data subject's interest in protection against violation of his/her personal integrity.

17. When personal data is collected from a data subject, the information regarding the LUXOFT GROUP entity collecting the information shall contain the name of the LUXOFT entity (i.e. the name of the controller) and address.

18. Such request shall be made in writing and shall be signed by the applicant.

19. Processing of personal data in the workplace with consent as legal ground shall be limited to situations where the employee is provided with a de facto choice of whether he/she should accept the processing or not and where the employee at a later stage may withdraw his/her consent without facing any negative consequences.

20. In general it is prohibited for others than public authorities to process personal data concerning legal offences involving criminal offences, judgments in criminal cases, coercive criminal procedural measures or administrative deprivation of liberty, even under circumstances where consent is obtained from the data subject. There are, however, exemptions to this prohibition; e.g. a controller may process such personal data concerning a data subject if (i) the processing relates to a single item of information which is necessary for the controller to process in order to determine, enforce or defend claims in an individual case or (ii) it is necessary for the compliance with a statutory notification requirement.

21. If LUXOFT GROUP wishes to keep the data for future recruitment needs, the candidate must be informed about this and give his/her consent.

22. It is generally not permitted to access employees' e-mails marked as private/personal. However, exceptions may apply when a serious suspicion of disloyal or criminal behaviour or a serious suspicion that the employee uses the IT equipment in violation of the employer's rules and guidelines exists.

23. The PDA does not impose requirements for implementation of specific security measures. The PDA only states that the controller shall implement appropriate technical and organisational measures to protect the personal data processed. Consequently, the controller needs to conduct an impact assessment in order to determine the appropriate level of protection. The measures taken shall provide a level of security that is appropriate having regard to (i) the technical possibilities available, (ii) what it would cost to implement the measures, (iii) the special risks that exist with processing personal data and (iv) the sensitivity of the personal data processed.

24. Before CCTV is introduced in a non-public area or in a public area you shall seek guidance from the relevant Data Protection Officer. The use of CCTV in non-public areas (e.g. in an office) (and in a public area) is subject to specific rules in the Swedish Camera Monitoring Act (2013:460) and the Swedish Camera Monitoring Ordinance (2013:463) and is only permitted under certain circumstances.

25. No specific maximum/minimum retention period applies for visitor registers, i.e. such records may not be kept for a longer period in time than is necessary having regard to the purpose of the processing. Consequently, the three (3) year period has to be justified with regard to the purpose of the processing.

18. SWITZERLAND

1. Under Swiss law, personal data includes all information that relates (either directly or indirectly) to an identified or identifiable individual or legal person (corporate entity). Foreign countries do not offer an adequate level of legal protection for personal data related to a legal person. The Swiss-US Safe Harbor scheme and the standard contractual clauses provided by the EU Commission do not include personal data related to a legal person. Additional protections for personal data may be necessary, as an amendment of the standard clauses.

2. Information shall be provided if sensitive data is collected.

3. It is usually not permitted to collect criminal conviction data unless the job specifically requires it (e.g. financial crimes for a cashier).

4. The unsuccessful applicant shall consent.

5. General monitoring of an employee's behaviour is not permissible (e.g. permanent monitoring of an employee's e-mail correspondence on a non-anonymous basis). With respect to the monitoring of the internet and/or e-mail use, permanent monitoring is permissible if such monitoring is based on anonymized log files (monitoring on a non-personal basis). Once a misuse has been discovered, the employer may then analyse the log file on a personal basis. In addition, the log files may be analysed on a personal basis if there are specific indications that there has been a breach of the rules by an employee. In any event, for such monitoring to be permissible, the respective employer must implement a monitoring policy which must be disclosed to the employees. Representatives of employees shall be consulted before the adoption of the policy.

6. The access to any e-mails clearly marked as private is prohibited and may even constitute a criminal offence.

7. Reference to the Federal Data Protection Act to be added.

19. UKRAINE

1. It was mandatory for companies to register databases containing personal data until 2014. Since 8 January 2014, companies are only required to notify the Ombudsman on the processing of personal data which are of particular risk to the rights and freedoms of an individual (pertaining to sensitive information or the so called 'risky data').

   At the beginning of this year 2014 the Ukrainian Parliament Commissioner for Human Rights (the Ombudsman) became the new regulatory authority. Having approved a new privacy compliance audit procedure, the Ombudsman is now authorised to perform data compliance audits. The privacy compliance audit procedure contains the rules governing audits and describes the types of the audits that may be undertaken (such as on-site or internal, scheduled or unscheduled). Following an audit, the Ombudsman or its authorised representative can issue an order for privacy compliance. This order is binding and failing to comply will give rise to liability.

2. According to the local legislation, 'risky data' includes data on: race, ethnic and national origin; political, religious or ideology beliefs; membership in political parties, trade unions, religious organizations or ideology NGOs; health; sexual life; biometrical data; genetic data; administrative or criminal liability records; criminal prosecution and police investigation measures; being victim of certain violence; personal location.

   When processing any categories of 'risky data', the data controller must notify the Ombudsman within 30 days from the date of starting the processing of such data. Notification may be carried out in different ways (e.g. by letter, e-mail, fax, etc.) and the Ombudsman has approved notification templates to streamline the procedure for data controllers. Companies that process 'risky data' about their employees (e.g. health records, temporary disability information) may be exempted from the notification procedures if that data is processed for employment purposes only.

3. Only information about the Personal Department responsible for protection of personal data relating to 'risky data' must be notified to the Ombudsman.

4. If you collect personal data about individuals, you must provide also the following information: name of LUXOFT entity and its location.

5. In Ukraine, when the LUXOFT GROUP collects personal information from an individual, it must also inform the individual of the location where the personal data are/will be kept.

6. According to the legislation of Ukraine, violation of personal data protection legislation is subject to an administrative liability. No criminal liability is prescribed by the law.

7. LUXOFT GROUP is entitled to process information about an individual without his/her consent when it is necessary to protect his/her vital interests, but up to the date when obtaining consent becomes possible. It is also recommendable to obtain consent for processing the data of job applicants.

8. Processing of information on criminal offence of an individual is a subject to notification the Ombudsman within 30 days from the date of starting the processing.

9. Use of data for a new purpose must always be informed to the individual and in certain cases consent must also be requested.

10. You must inform the unsuccessful applicants that you want to keep CVs on file for future use and CVs should only be retained if the applicants give their explicit consent on such.

20. USA

1. There are strict limitations regarding the use of criminal background checks, which vary by state and even down to local city ordinances. Before applicants are requested to provide such information, legal advice must be obtained for the specific request.

2. Generally notice is not required under U.S. law.

3. An employee in the U.S. is not required to explicitly consent to the gathering of their personal data for employment purposes.

4. Employees should be told clearly whether their electronic communications will be monitored and how.

5. Retention of HR records in the United States is governed by both federal (FED) and state law. Luxoft offices located in California Connecticut, Illinois, Indiana, Michigan, New Jersey, New York, North Carolina, South Carolina, Tennessee, Texas and Washington may have different statutory requirements as indicated in this matrix. In some instances there were several laws within the same jurisdiction that imposed different record retention periods; in this case we used the longest period in the matrix. If the state and federal retention periods differ, employer must comply with the jurisdiction that requires the longest retention period. This matrix does not include local city ordinances that may apply. For example, New York City and San Francisco city may have different retention periods.

21. VIETNAM

1. LUXOFT GROUP may only process personal data where it has a lawful purpose for this and after obtaining prior consent from the relevant individual (in Vietnam: “data owner”).

2. Generally, staff may collect and process personal data (1) after consent from the relevant individual (in Vietnam: “data owner”) has been given and (2) process the personal data for the purposes and store it only for a given period of time as agreed by the relevant individual.

3. In addition, LUXOFT GROUP must provide information about the form, scope, place and period for storing the information.

4. In addition to accessing and correcting, Vietnam law allows individuals to cancel (i.e. delete) their personal information which is stored on a network.

5. In Vietnam, LUXOFT GROUP should not process information about applicants and employees without their consent.

6. Where LUXOFT GROUP provides staff data to third parties to provide benefits, make staff aware of this in the literature used to explain the benefits (e.g. pension, insurance or private health providers) and ensure that consent from each employee has been provided. If LUXOFT GROUP collects information to pass on to the third parties for whatever purpose, do ensure that consent from each employee has been obtained.

7. References: always check with the employee and ensure that his/her consent has been obtained before providing a reference.

8. The Head of Personnel Department must authorise any requests to monitor specific employees. This would apply to any of monitoring IT Equipment and traffic on the IT Network telephone calls and other forms of monitoring. Before authorising any monitoring, the Head of Personnel Department shall – in addition to the other requirements listed – ensure that consent from such employee has been obtained.

22. HONG KONG

1. LUXOFT GROUP should follow the Data Protection Principles which represents the core of the Ordinance covering the life cycle of a piece of personal data:

- Personal data must be collected in a lawful and fair way, for a purpose directly related to a function /activity of the data user. Data subjects must be notified of the purpose and the classes of persons to whom the data may be transferred.
- Practicable steps shall be taken to ensure personal data is accurate and not kept longer than is necessary to fulfil the purpose for which it is used. A data user needs to take practicable steps to safeguard personal data from unauthorised or accidental access, processing, erasure, loss or use.
- Personal data must be used for the purpose for which the data is collected or for a directly related purpose, unless voluntary and explicit consent with a new purpose is obtained from the data subject.
- A data user must take practicable steps to make personal data policies and practices known to the public regarding the types of personal data it holds and how the data is used.
- A data subject must be given access to his/her personal data and allowed to make corrections if it is inaccurate.

1. Currently, there is no requirement for the registration of data users, to appoint a data protection officer, no restrictions for transfer of personal data outside of Hong Kong, no mandatory legal requirement for data users to notify authorities or data subjects about data breaches.

2. A data user may collect personal data from data subjects if:

- the personal data is related to a function of the data user
- the collection is necessary, lawful and fair
- the data collected is not excessive, and
- the data user has been informed of the following:
- whether the provision of personal data by data subjects is mandatory and the consequence(s) for not
- supplying the data
- the purposes for which the data will be used
- the persons to whom the data may be transferred
- the data subjects’ right to request for access and/or correction their personal data, and
- the contact details of the person to whom requests for access or correction should be sent.

3. Data users may not transfer personal data to third parties, unless the data subjects have been informed of the following before their personal data was collected:

- that their personal data may be transferred
- the classes of persons to whom the data may be transferred.

4. The direct marketing provisions generally require data users who wish to either use or provide personal data for direct marketing purposes to make specific disclosures to the data subjects and obtain consents for such actions. The disclosures include:

- a statement of intention to use/provide their personal data for direct marketing
- a statement that the data user may not use/provide the personal data without the data subjects' consent
- a dedicated channel via which the data subjects may give such consent
- the kind(s) of personal data to be used/provided
- the class(es) of persons to whom the personal data may be provided
- the class(es) of goods/services to be direct marketed, and
- a statement that the personal data may be provided for gain, if applicable.

Furthermore, if the consent was given orally, data users have the additional obligation to send a written confirmation to the data subject confirming the particulars of the consent received. In addition, when data users use personal data for the purposes of direct marketing for the first time, they must inform the subjects that they may opt-out at any time, free of charge.