NEW YORK STATE BAR ASSOCIATION

INTERNATIONAL SECTION

Seasonal Meeting 2018

October 23 – 26, 2018

Montreal, Canada

PANEL 1

Sharing Employee Data Across Borders and GDPR: Pitfalls and Practicalities

CO-CHAIRS

François Joli-Couer, Borden Ladner Gervais LLP, Montreal, Canada

Rodrigo Solá Torino, Marval O'Farrell & Mairal, Buenos Aires, Argentina

PANELISTS

Erica Schohn, Skadden, Arps, Slate, Meagher & Flom LLP, New York

Filip Saelens, Loyens & Leoff N.V., Belgium

Warren Chik, Singapore Management University, Singapore

Sharing Employee Data Across Borders and GDPR:
Pitfalls and Practicalities

The Asian Perspective

Assoc. Prof Warren Chik, SOL, SMU

1. Introduction to the Asian Data Protection Regime and Trends
2. The Employer-Employee Relationship and the Singapore Personal Data Protection Act
    a. Data Protection in the Employment Context and Relationship
    b. Obligations and Cross-Border Dataflow Implications

1. Introduction to the Asian Data Protection Regime and Trends

Unlike the EU, there is no consistency to the prescription, form and substance in Asian data protection laws. Although the APEC Privacy Framework have provided some impetus for the enactment of such laws, or at least voluntary self-regulation or standard setting in the domestic context by the public and private sectors in some cases, the laws have emerged gradually and in phases, in accordance with the political and socio-economic context of each jurisdiction.

Nevertheless, there is an accelerating momentum to these laws in recent years for several reasons including trade, economic, political and social growth and changes. The pressure from countries with more matured and advanced data protection laws, especially the EU, and the threat of the stemming of dataflow as well as increasing security concerns have led to this. In fact, some data protection laws are a part of cybersecurity laws in some countries like India and China. In Singapore, the government policy to develop a data hub and the Smart Nation initiative, which is increasingly replicated in other Southeast Asian countries, is an additional accelerant for the development and growth of data protection laws.

However, the approach is generally not one based on privacy as a fundamental right but a pragmatic one that is more related to a balancing of interest between individual rights and business needs.[1]

2. The Employer-Employee Relationship and the Singapore Personal Data Protection Act

[1] For example, see section 3 of the Singapore PDPA, which states that: "The purpose of this Act is to govern the collection, use and disclosure of personal data by organizations in a manner that recognizes both the right of individuals to protect their personal data and the need of organizations to collect, use or disclose personal data for purposes that a reasonable person would consider appropriate in the circumstances."

Singapore's Personal Data Protection Act of 2012 (PDPA), which Data Protection provisions entered into effect on 2 July 2014, protects an individual's personal data, defined as "data, whether true or not, about an individual, who can be identified from that data, either on its own or together with other information to which the relevant organisation has or is likely to have access."[2]

There are two perspectives to note here. First, the employee is an "individual" or data subject for the purpose of the PDPA in relation to the employer that is the "organisation" or data controller. Second, within that employee-employer relationship, the employee is in a position to perform functions for the employer that relates to third party personal data; as such, the Act provides for the protection of employees from liability under the PDPA when "acting in the course of his employment with an organisation".[3]

2a. Data Protection in the Employment Context and Relationship

This study will include employees in an organization, which in Singapore includes an employee for remuneration (i.e. paid) or a volunteer (see Section 2). The obligations will apply, but specifically in the employment context and the specific and special relationship between an employer and an employee that is different from the usual business and consumer relationship and the like. Some of these include the following:

1. Employees are given immunity when "acting in the course of his employment with (i.e. on behalf of) an organization. This is provided for under section 4(1)(b) of the PDPA and neither address the issue of the assessment of liability between the parties and with third parties under contract law nor apply the agency principles as such.[4] The PDPA offers baseline protection and defers to other laws where they provide for stronger protection or where there is a conflict (which can include employment law; see section 4(6)(a) & (b) respectively).

2. There are exemptions from the consent obligation on employers for collection, use and disclosure of personal data of an employee under certain circumstances –

[2] Section 2 of the Singapore PDPA.
[3] Section 4(1)(b) of the Singapore PDPA. There is concomitantly an additional a defense for employees from offences relating to digital marketing under the Singapore PDPA provisions on the Do Not Call Registry regime. Section 48(1) of the Singapore PDPA provides a defense for "any employee in respect of an act or conduct alleged to have been done to engaged in, as the case may be, by the employee … [if it is proven] that he did the act or engaged in the conduct in good faith in the course of his employment; or in accordance with instructions given to him by or on behalf of his employer in the course of his employment."
[4] Section 53(1) provides for liability of employers for the acts of their employees. It is provided that: "Any Act done or conduct engaged in by a person in the course of his employment (referred to in this section as the employee) shall be treated for the purposes of this Act as done or engaged in by his employer as well as by him, whether or not it was done or engaged in with the employer's knowledge or approval." The employer is generally liable for the acts of the employee in the course of employment unless practicable steps were taken to prevent the employee from doing such acts or engaging in such conduct (under subsection (2)).

a. The personal data "is about an employee" that "is collected by an organization, being a party or a prospective party to a business asset transaction with another organization, from that organization" and that "relates directly to the part of the other organization or its business assets with which the business asset transaction is concerned".[5] This may have cross-border effect or implications if the transaction is between entities with a business presence in Singapore and another (or several other) countries.

b. "[T]he personal data is collected by the individual's employer and the collection is reasonable for the purpose of managing or terminating an employment relationship between the organization and the individual".[6] Also, an "evaluative purpose" includes for the purpose of determining the suitability, eligibility or qualifications of the individual to whom the data relates for the employment or for appointment to office; for promotion in employment or office or for continuance in employment or office; for removal from employment or office".[7]

c. "[T]he personal data was disclosed by a public agency, and the collection is consistent with the purpose of the disclosure by the public agency".[8] This is unique to Singapore and only a few other countries and may have implications for cross-border transfer into Singapore of foreign employee data.

d. If there are any other reasons under the Schedule such as necessary for the interest of the employee; "publicly available" information including data put on employment application databases, job search or headhunting websites that have already sought consent); necessary for evaluative purposes such as promotion and job performance review; debt related, which can include salary disputes; etc. This may also apply to exemption from consent in relation to use and disclosure (on top of collection), as the case may be and where so provided.[9]

e. If it is reasonable and appropriate under the circumstances not to seek consent generally; if the data is collected before the PDPA entered into effect; and if the deemed consent provision applies (which are different from the GDPR standards for consent).

[5] Para. 1(p) of the Second & Fourth Schedules read with Section 17 of the PDPA. This exception is subject to conditions and limitations under para. 3, mainly subject to necessity and terms of the business purchase agreement solely for purposes related to the business asset transaction as well as subject to the original purpose and retention limitations and notification requirements.
[6] Para. 1(o) of the Second Schedule read with Section 17 of the PDPA.
[7] Para. 1(f) of the Second & Third Schedules and para. 1(h) of the Fourth Schedule read with Section 17 of the PDPA.
[8] Para. 1(q) of the Second read with Section 17 of the PDPA. Query on disclosure by the employer to a public agency, which is not covered by the Act.
[9] See the specific exemptions under the Second to Fourth Schedules of the PDPA. See also the exemptions under the Fifth & Sixth Schedules on relevant exceptions from access and correction respectively.

f. If subsequent exemptions are made by the Minister or added to the Act by later amendments (e.g. the Public Consultation on Approaches to Managing Personal Data in the Digital Economy issued in July 2017 by the PDPC include as part of a set of proposed amendments a "legal and business purpose" exemption with conditions as well as 'notification only' exemptions).

3. Employees have contractual (confidential agreements, restraint of trade clauses, consent for collection, use and disclosure of personal data in the employment context such as for employment, evaluation, assessment, review, etc.) and common law obligations (including the law on confidence) to the employer, in particular for the maintenance of confidentiality of the employer's data and on the ownership, possession and control of that data, which incidentally can include the personal data of third parties with whom the employee may come in contact with or transact on behalf of the employer.

The usual obligations will apply to an employee's personal data that are not exempted. These include using the records for purposes only to the extent that it is reasonable and appropriate under the circumstances;[10] providing for protection of employee records using "reasonable security arrangements" and so on. The PDPA provides for a right of private civil action if an employee suffers loss or damage due to the contravention of these obligations.[11]

There are specific rules on the handling of employee and the employer-employee context that are unique to the relationship. For example, personal data may be involved in the following:

1. Office access and computer access security measures;
2. Office security measures (inc. surveillance);
3. Ownership of original works (i.e. copyright issues);
4. Employment benefits (e.g. address, overseas accommodation and travel information, criminal records, health records, etc.);
5. Legal requirements (i.e. employment and other laws);
6. Business and personal contact information;
7. Payment related matters (credit rating, etc.); and
8. Other human resource matters.

2b. Obligations and Cross-Border Dataflow Implications

For an employer, the data protection concerns and obligations relating to the protection of personal data of employees can depend on the nationality, residency and other factors. It could also depend on the place of business and/or where the employees' data is processed.

1. If employee data, with or without other personal data, are processed or in any way collected, stored, used or shared in another country, there are also cross-border implications and considerations. This can be to data

[10] Section 18 of the Singapore PDPA.
[11] Section 32 of the Singapore PDPA.

intermediaries/processors such as cloud technology services and the like. See Table 1.

2. For employees that are the nationals of other countries, is resident in another country (for work or otherwise, such as in a remote or long distance work arrangement), the territorial rules of other countries' data protection laws may extend the applicable law and jurisdiction to the employer-employee relationship. Similarly, if there is impact or effects, or the purpose relates to another jurisdiction, other laws may apply. See Table 1.

3. There are also mandatory breach reporting obligations that are being proposed in the next amendment to the PDPA under the Public Consultation on Approaches to Managing Personal Data in the Digital Economy issued in July 2017 by the PDPC. This relates to Singapore law and other countries may have similar requirements too.

Although the Singapore PDPA does not have a jurisdictional clause to establish a 'Singapore link', the territorial scope seems extensive given the definitions of "organization" that "includes any individual, company, association or body of persons, corporate or unincorporated, whether or not formed or recognized under the law of Singapore; or resident, or having an office or a place of business, in Singapore"; and "individual" which merely refers to a "natural person, whether living or deceased".[12]

Table 1. Transborder Data Flow and Territorial Scope

Type of Organization Data Subject	Data Controller/ Organization	Data Processor/ Intermediary
Local Employee	Singapore PDPA applies	Singapore PDPA exempts except for the protection and retention obligations[13]
Foreign Employee	Singapore PDPA applies Other countries' laws may apply	Singapore PDPA exempts except for the protection and retention obligations[14] Other countries' laws may apply

Insofar as transfer obligations are concerned, the common requirement is that an organization "shall not transfer any personal data to a country or territory outside Singapore except in accordance with requirements prescribed under" the PDPA to "ensure that organizations provide a standard of protection to personal data so transferred that is comparable to [or stronger than] the protection under this Act".[15]

[12] Section 2 of the Singapore PDPA.
[13] Section 4(2) of the Singapore PDPA. The definition of a "data Intermediary" for this limited application of the Act may not be the same as the equivalent in other countries.
[14] Section 4(2) of the Singapore PDPA. The definition of a "data Intermediary" for this limited application of the Act may not be the same as the equivalent in other countries.
[15] Section 26(1) of the Singapore PDPA states that "An organization shall not transfer any personal data to a country or territory outside Singapore except in accordance with requirements prescribed

The transferring organization will remain responsible for the personal data in its possession and control or that is processed on its behalf or for its purposes by a data intermediary (in Singapore or overseas).[16]

The following are some of the regional and/or international arrangements that can address cross-border data flow concerns as well as improve and facilitate trans-border data flow arrangements:

1. Forming recognition arrangements like the EU-US Privacy Shield that can perhaps be replicated elsewhere and adequacy findings and white lists;[17]
2. Participation in the APEC Framework and the Cross-Border Privacy Rules (CBPR) and Privacy Recognition for Processors (PRP) Systems;[18]
3. The development and use of TRUSTe, Trust Marks certifications and privacy seals;[19] and
4. Working data protection obligations into bilateral and multi-lateral trade discussions.[20] Perhaps even mutual recognition agreements (such as trustmarks, privacy seals or even generally) specific to data protection can be explored.

Proper internal processes are also important including, for example:

1. Consent for data transfer and the use of model clause agreements;[21]
2. The use of data transfer agreements to comply with the PDPA (when transferring out) and other countries' laws (when transferring in);[22] and

---

under this Act to ensure that organizations provide a standard of protection to personal data so transferred that is comparable to the protection under this Act." There are also regulations and subsidiary legislation on the matter including the Personal Data Protection Regulations of 2014 and the Personal Data Protection (Enforcement) Regulations of 2014.

[16] Section 4(3) of the Singapore PDPA.

[17] PDPC advisory guidelines setting out the criteria for such assessment can also be helpful. This can be done generally or sectorally, as the PDPC has done sector-specific guidelines as well.

[18] Singapore announced its participation in the APEC CBPR and PRP systems through a Notice of Intent in July 2017, and approval was granted by the Joint Oversight Panel on 20 February 2018.

[19] In Singapore, the National Trust Council's trustmark "TrustSg" is publicly supported by the Infocomm Development Authority. The next step will be a new data protection trustmark which, when it comes to fruition, will support certification of key products and services as well as organizational compliance.the PDPC is developing a data protection trustmark certification scheme, to be aligned with the APEC CBPR and PRP systems, which is anticipated for late 2018 or early 2019.

[20] Data protection laws vis-à-vis trade rules are sometimes defined in trade pacts such as the one between the EU and Singapore (EUSFTA) in Article 8.62 "General Exceptions" and India and Singapore in the Comprehensive Economic Cooperation Agreement (ISCECA) in Article 7.21 in Chapter 7 "Trade in Services" wherein data protection is required not to be "applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination against the other Party, or a disguised restriction" on the establishment or cross-border supply of services and trade in services respectively. This is in order not to conflict with trade obligations. Similar provisions also appear in the Japan-India Comprehensive Economic Partnership Agreement. See also, the Singapore-Australia, Japan-Singapore. Also, a similar understanding extends to other types of trade obligations such as financial services, e-commerce and customs-related matters. In contrast, trade agreements with countries that do not have fully formed data protection laws lack similar provisions, such as that with China.

[21] However, consent cannot be obtained to circumvent section 26(1) of the PDPA. See regulation 9(4) of the PDP Regulations. Instances of one-off transfers may be made according to regulation 9(3) of the PDP Regulations.

3. The appointment and function of a Data Protection Officer in any organization.

Threats to smooth flow of data across borders include:

1. Trend in some countries to data localization laws; and
2. The network of inconsistent principles and laws that still exists outside the EU GDPR bloc.[23]

References:

- APEC Privacy Framework and Cross-Border Privacy Rules < http://www.cbprs.org/ >
- ABLI Data Privacy Project on Convergence of Rules and Standards in the Area of Cross-Border Data Transfers in Asia < http://abli.asia/PROJECTS/Data-Privacy-Project >
- Hannah Lim, Data Protection in the Employment Setting, in Chesterman ed., Data Protection Law in Singapore - Privacy and Sovereignty in an Interconnected World (2ed 2018 Academy Publishing)
- Alan Charles Raul ed., The Privacy, Data Protection and Cybersecurity Law Review (4ed 2017)
- Graham Greenleaf, Asian Data Privacy Laws: Trade and Human Rights Perspectives (2014 Oxford University Press)

[22] Legally enforceable obligations include contractual agreements to ensure that the overseas recipient is legally bound and obligated to provide a comparative standard of protection. It also offers the transferring party remedies if it is bound by the infringement by the recipient-transferee. Another method is the use of Binding Corporate Rules (BCR).

[23] Unable to transfer employee data out of the country; having to understand and comply with peculiar local requirements including sensitive employee personal data; having to use in-country (and possible less preferred and separate) data processors such as for payroll; difficulties conducting cross-border investigations; difficulties in using shared services such as online intranet services; etc.

The labor relations and the implementation of the General Data Protection Regulation (GDPR) in Belgium

Filip Saelens,
Loyens & Leoff N.V.,
Belgium

1. Implementation of GDPR in Belgium. Personal data and privacy rules.

The Belgian implementation act of the General Data Protection Regulation (GDPR) was published in September 2018 without any specific HR provisions.

GDPR considers personal data as any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Sensitive personal data is personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. Personal data relating to criminal convictions and offences or related security measures is also considered sensitive. Sensitive personal data enjoy an even stronger protection under the GDPR, whereby processing is in principle prohibited, unless an exception applies.

Non-compliance with the provisions of the GDPR shall be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 2 or 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

2. Employer – Employee Relationship

2.1. Restrictions on monitoring employees in Belgium

National Collective Bargaining Agreement No. 81 (CBA No. 81) allows employers to monitor the use of e-mail and the Internet during working hours, provided that a number of conditions are met, as follows:

- The monitoring should serve one of the purposes defined by the agreement. These purposes are limited by CBA No. 81 to the following:
  (1) the prevention of wrongful or defamatory acts;
  (2) the protection of the company's economic and financial interests;

(3) the security and proper functioning of the company's IT network; or
(4) ensuring employee compliance with the company's IT policy.

- The monitoring should be proportional to its purposes.

- Prior to implementing the monitoring, all employees concerned should be informed collectively (through their representative bodies) and individually of the fact that monitoring may occur and for what purposes.

Yet even if some of these conditions are not complied with, evidence obtained through unlawful monitoring is in certain cases still accepted by the courts.

2.2. Employees Data Access

The general principles of the GDPR will apply. The data subject has the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

(a) the purposes of the processing;

(b) the categories of personal data concerned;

(c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries;

(d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

(e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

(f) the right to lodge a complaint with a supervisory authority;

(g) where the personal data are not collected from the data subject, any available information as to their source;

(h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) 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 the data subject.

The controller should provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. The right to obtain a copy may not adversely affect the rights and freedoms of others.

2.3. Sharing Employee Data with Third Party Service Providers

A controller may use only processors providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing

will meet the requirements of the GDPR and ensure the protection of the rights of the data subject.

The processor may not engage another processor without prior specific or general written authorization of the controller.

Processing by a processor shall be governed by a contract that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:

(a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organization,

(b) ensures that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(c) takes all measures required to ensure the safety of the data;

(d) respects the conditions for engaging another processor;

(e) taking into account the nature of the processing, assists the controller by appropriate technical and organizational measures for the fulfilment of the controller's obligation to respond to data subject requests;

(f) assists the controller in ensuring compliance with the obligations pursuant to the GDPR;

(g) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies;

(h) makes available to the controller all information necessary to demonstrate compliance and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract shall be imposed on that subprocessor by way of a contract. Where the subprocessor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of subprocessor's obligations.

2.4. Restrictions on Transferring Data Overseas

The GDPR permits personal data transfers to a third country subject to compliance with set conditions, including conditions for onward transfer.

The GDPR allows for data transfers to countries whose legal regime is deemed by the European Commission to provide for an “adequate” level of personal data protection.

In the absence of an adequacy decision, however, transfers are also allowed outside non-EU states under certain circumstances, such as by use of standard contractual clauses or binding corporate rules (BCRs). Derogations are also permitted under limited additional circumstances. Finally, a newly introduced scheme allows for transfers based upon certifications, provided that binding and enforceable commitments are made by the controller or processor to apply the appropriate safeguards.

3. Employee Privacy and Transactions

Employee data can be shared with a potential buyer before a transaction according to article 6(f) of the GDPR (“promotion of the legitimate interests of the controller”). The general rules of adequacy, relevance and proportionality apply. Information should only be disclosed on a need-to-know basis and redacted in such a way that the employees may not be identified. Working in phases where more sensitive information is only disclosed to the potential buyer after a preliminary selection (e.g. in a bidding process) is also recommended to ensure proportionality.

Once the sale is complete, the buyer has a legitimate interest to receive all relevant employment data

The Employee Privacy and Data Protection in Canada

François Joli-Coeur
Borden Ladner Gervais LLP
Canada

1. Employee privacy

1.1. Privacy rules to protect employees' data in Canada.

In Canada, private sector organizations are regulated by four privacy statutes laws:

Federal: Personal Information Protection and Electronic Documents Act, S.C. 2000, c.5 ("PIPEDA"). This law applies to federally-regulated organizations (e.g. banks, airlines, railway companies) and provincially-regulated organizations in provinces that have not adopted a privacy statute recognized as substantially similar to PIPEDA. The three following provinces have adopted such statute:

- Alberta: Personal Information Protection Act, S.A. 2003, c. P-6.5 ("Alberta PIPA")

- British Columbia: Personal Information Protection Act, S.B.C. 2003, c. 63 ("BC PIPA")

- Quebec: An Act Respecting the Protection of Personal Information in the Private Sector, R.S.Q., c. P-39.1 ("Quebec Private Sector Act")

PIPEDA only applies to the collection, use and disclosure of personal information of employees by federally regulated employers. Provincially regulated employers are only subject to the provincial privacy laws above (in Alberta, British Columbia and Quebec). In the remaining provinces, however, it is considered a best practice to follow the federal PIPEDA.

1.2. Private and sensitive personal data in Canada.

"Sensitive personal information" is not defined under the four Canadian privacy laws. PIPEDA indicates that while some information (for example, medical records and income records) is almost always considered to be sensitive, any information can be sensitive, depending on the context. In an employment context, an employee's browsing history on its work computer could be considered sensitive information because it could reveal this employee's lifestyle.

In general, Canadian privacy laws provide that the appropriate security safeguards to protect personal information depends on its sensitivity. The appropriate form of consent (opt-in/express vs. opt-out/implied) may also vary according to the sensitivity

of the information. For instance, organizations need express consent if they want to use sensitive personal information for secondary purposes.

1.3. Penalties for breaching privacy rules and Restrictions on keeping employee records.

Individuals may seek damages in a civil court. Some privacy commissioners in Canada can issue fines for any breaches of the statute, while others are limited to making findings or whether or not a particular complaint is founded or not. Under PIPEDA, once that finding is made, if the individual is not satisfied with the outcome, he or she can apply to the federal court for damages, but this is rarely done and the damages are relatively small. Generally, where the legislation applies, there are fines for purposely obstructing an investigation or deleting information that was subject to an access request, among other intentional breaches.

Organizations must retain personal information only for so long as it is needed to fulfill the purpose for which was collected, after which they must be destroyed, erased, or made anonymous. Organizations should develop guidelines and implement procedures with respect to the retention of personal information. These guidelines should include minimum and maximum retention periods. Personal information that has been used to make a decision about an individual shall be retained long enough to allow the individual access to the information after the decision has been made. An organization may be subject to legislative requirements with respect to retention periods (depending on the province and other circumstances).

2. HR Issues/Sharing Employee Data

2.1. Restrictions on monitoring employees in Canada

Under PIPEDA, the Alberta PIPA and the BC PIPA, employers may collect, use and disclose personal information about employees that is required to establish, manage or terminate an employment relationship between the organization and that individual. However, they must inform the employees of such activities. This could cover monitoring employees, provided that this monitoring is for the purpose of managing/terminating the employment relationship.

In Quebec, there is no such rule. Quebec law provides that organizations must obtain consent for the collection, use and disclosure of personal information, including for employees, and that such consent must be “manifest, free, and enlightened.” In practice, many organizations are transparent about their monitoring practices with their employees, for instance through internal privacy policies and do not require that employees sign the privacy policy, but they ask employees to sign a document acknowledging that they have received a copy of the policy and read it. This is likely sufficient for the organization to argue that it has obtained consent to use the employees’ personal information for purposes that are reasonably related to the employment relationship.

2.2. Rules that apply to employee’s access to data held about them.

Employees have a right to access the personal information their employer holds about them. The four laws provide for certain exceptions to this right, which differ slightly (e.g. when the information is prohibitively costly to provide, information that contains references to other individuals, information that cannot be disclosed for legal, security, or commercial proprietary reasons, and information that is subject to solicitor-client or litigation privilege).

2.3. Sharing employee data with third party service providers

Employers remain responsible for the personal information of their employees even when this information is transferred to a service provider for processing. Employers must therefore enter into a contract with the service provider to ensure the protection of the information when it is under the custody of the service provider. Such contracts are usually expected to include clauses requiring the service provider to maintain information protection practices and procedures that comply with industry best practices, to comply with all applicable Canadian legal requirements, to maintain adequate training programs, to ensure the employees' data is only accessed on a need to know basis, to notify the employer in the case of a data breach.

Where an organization uses a service provider outside of Canada to collect, use or disclose personal information of Albertans, the organization must (i) notify individuals how they can obtain information about the organization's policies and practices with respect to the use of service providers outside of Canada, including the name, position or title of a person who is able to answer questions on behalf of the organization, and (ii) include in its privacy policy or in a separate document, the countries outside of Canada in which the collection, use or disclosure of personal information may occur and the purposes for which the service provider outside of Canada has been authorized to collect, use or disclose personal information on behalf of the organization.

2.4. Restrictions on transferring data overseas.

Under Canadian law, the cross-border transfers of personal information is permitted as long as: the organization transferring the data "uses contractual or other means to provide a comparable level of protection while the information is being processed" by the other organization outside Canada and individuals whose information will be transferred outside Canada are notified of such transfer and that their personal information will, as a result, be subject to the laws applicable there (such that governmental and regulatory authorities in these jurisdictions may access their information under orders issued in these foreign jurisdictions).

There are particular requirements under the Alberta PIPA: an organization that uses a service provider outside Canada to collect, use, disclose or store personal information on its behalf must include in its privacy policy, which must be available on request, 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. The organization

must also notify the individual of the way in which the individual may obtain access to written information about the organization's policies and practices with respect to service providers outside Canada, and the name or position name or title of a person who is able to answer on behalf of the organization the individual's questions about the collection, use, disclosure or storage of personal information by service providers outside Canada.

3. Employee Privacy and Transactions

3.1. Sharing employee data with a potential buyer before a transaction is signed.

Under PIPEDA, the Alberta PIPA and the BC PIPA, there is a consent exception for the sharing of personal information in the context of a potential business transaction. The following conditions must be met:

- the personal information is necessary to determine whether to proceed with the transaction and to complete the transaction;

- the disclosure is governed by an agreement between the organization and the proposed buyer that contains certain specified provisions regarding the use/disclosure, protection and return/destruction of the personal information; and

- if the proposed transaction does not proceed, the proposed buyer returns/destroys all of the disclosed personal information.

Under PIPEDA, the Alberta PIPA and the BC PIPA, there is a consent exception for the sharing of personal information in the context of a potential business transaction. The following conditions must be met:

- the personal information is necessary for carrying on the business or activity that was the subject of the transaction;

- the disclosure is governed by an agreement between the organization and the buyer that contains certain specified provisions regarding the use/disclosure and protection of the personal information and obligates the buyer to give effect to an individual's withdrawal of consent; and

- within a reasonable time after the transaction is completed, either or both of organizations and the buyer give notice to the individuals whose personal information is disclosed/used that the transaction has been completed and that their personal information has been disclosed to the buyer.

The protection of personal data on labor relationships in Argentina and the effect of the GDPR

Rodrigo Solá Torino
Marval O'Farrell & Mairal,
Buenos Aires, Argentina

1. Introduction

The primary law governing personal data protection and security in Argentina is Law No 25,326 on Protection of Personal Data ('Personal Data Protection Law', or PDPL). Decree No 558/2001 provides the primary regulations implemented under the PDPL. The purpose of the PDPL is the comprehensive protection of personal information recorded in public and private databases and to guarantee the right of individuals to protection of their honor and privacy, as well as the right to access that information in accordance with Article 43 of the Constitution.

One of the most significant aspects of the PDPL is that it extends protection to data belonging to legal entities. The PDPL does not provide any rule on which specific provisions apply to companies; thus, it could be reasonably argued that, in general, any provision of the PDPL will apply to the protection of companies' personal data, or it could be concluded that regulations concerning sensitive data (information pertaining to the data subject's racial or ethnic origin; political opinions; moral, religious or philosophical views; trade union affiliations; health; or sex life) would not apply, as this kind of data cannot be associated with a legal entity. Article 27 of the PDPL addresses data with promotional, commercial or advertising purposes, including processing of data that allows a data subject's consumer habits to be accessible, that has been provided by the data subject or has been obtained with their consent.

The data subject can exercise a right of access to these databases free of charge and may request withdrawal or blocking of their name from any databases used for these advertising-related purposes.

Regulation No 4/2009 of the Personal Data Protection Act (PDPA) reinforced the 'opt-out' language required by Article 27(3) by requiring that specific opt-out language be included in each communication with marketing purposes. In addition, unsolicited marketing emails must state 'Advertisement' in the subject line. Non-criminal violations of an individual's privacy and dignity, such as by divulging correspondence or publishing their images without consent, are punishable under Article 52 of the Civil and Commercial Code (CCC) by an injunction against the offending activities and/or by compensation for damages, as determined by a judge. Criminal violations of the right to personal honor may arise when false information is spread about an individual (Criminal Code subsection 109–11). Data controllers must take technical and organizational measures to guarantee the security and confidentiality of their data (PDPL section 9). In securing and maintaining data and

associated databases, the data controller must keep records on incidents related to security faults.

PDPA Rule 60 - E/2016, published in the Official Gazette on 18 November 2016, sets forth aspects concerning the international transfer of personal data. Pursuant to the PDPL, the transfer of personal data to countries that have not enacted adequate legislation on personal data protection is forbidden. The PDPA Rule 60 lists the countries with an adequate protection, similar to those recognized by the EU.

Furthermore, Rule 60 approved two sets of standard model clauses for data controller–data controller transfers, as well as data controller–data processor transfers. Both model clauses were based on the EU Model Contracts for the transfer of personal data to third countries approved by Decisions 2001/497/EC and 2010/87/EU.

In the event that the parties opt to use a different model for the data transfer to countries with inadequate protection, or the agreement does not reflect the principles, safeguards and content related to personal data protection provided in the standard model clauses, then such agreement will need to be submitted to the PDPA for approval within 30 calendar days from its execution. Before Rule 60 was issued no approval was required. The PDPA invited academic institutions, companies, individuals and civil rights associations in May 2016 to review and discuss the potential amendment to the current law on data protection intended to align it with the GDPR.

2. Recent Updates in Data Protection in Argentina

On September 18, 2018, the Argentine Executive Brach introduced a bill intended to replace Personal Data Protection Law No. 25,326 (the “Law”), enacted in 2000.

The Bill highlights the need to replace the current Law based on the fact that is has become outdated in comparison to the technological and legal developments, especially regarding the passing of the European General Data Protection Regulation (the “GDPR”).

The most significant changes include the following:

- The Bill introduces new definitions aligned with the EU regulations, such as the concept of data base, personal data and sensitive data. At the same time, the Bill introduces new concepts regarding genetic data, biometric data, economic group, security incidents and international transfer.

- The Bill limits the scope of the concept of data subjects to human persons. Therefore, legal entities are excluded from the scope of the Bill.

- The Bill introduces new grounds for the collection and processing of personal data different to consent, such as legitimate interest.

- The Bill widens the protection of data by stating that the purpose of the law will be the comprehensive protection of personal data, and not limiting it —as the Law currently does— to the personal data included in data base, either private or public, aimed at preparing reports, so as to guarantee the full enjoyment of subject data's rights.

- The Bill introduces the concept of accountability as a general principle for the fulfillment of the obligations that arise from the law in line with most international data protection laws.

- The Bill updates data subjects' rights by including the right to oppose to the processing of their data, the right to oppose to be subject of a decision made being based on the automatized processing of their data, the right to data portability, by which the subject data is able to request to the data controller a copy of the personal data subject to the processing, and the right to request their data to be transferred to another company, if technically feasible.

- The Bill introduces the obligation to report to the controlling authority and data subjects any security incident.

- The Bill introduces the Data Protection Delegate, who will carry out specific functions.

- The Bill introduces new provisions regarding sensitive data so as to bring more clarity to those in charge of dealing with such category of data.

- Regarding the international transfer of personal data, the Bill introduces the cases when such transfer is legal.

- The Bill introduces the obligation of the data controller to conduct impact evaluations in those cases in which the nature, scope, context and purpose of the treatment of data may affect data subjects' rights.

- The Bill introduces an increase in the penalties for infringement.

3. Recent Updates in Data Protection in Latin America

3.1. Brazil

Brazilian General Data Protection Law (*Lei Geral de Proteção de Dados* - "LGPD"), Law No. 13.709/18, was published in August 14, 2018 and will become effective in February 2020. It regulates the processing of personal data, including by digital means, by a natural person or legal entity governed by public or private law, for the purpose of protecting the essential rights of freedom and privacy and the free development of the personality of the individuals.

Brazilian LGPD is very similar to the European GDPR, in most ways, especially in what concerns the legitimate and proportional use of information being processed by the company, transparency (considering the motives for processing and the access of the data subject/owner to the information being processed), security and retention of information (meaning the data should be deleted when no longer needed).

In its article 3, the Law sets forth that it "applies to any processing operation carried out by a natural person or legal entity governed by public or private law, irrespective of the means, of the country in which its headquarter is located or of the country in which the data are located", provided that:

i. the processing operation is carried out in the Brazilian territory;

ii. the purpose of the processing activity is the offer or supply of goods or services or the processing of data of individuals located in the Brazilian territory;

iii. the processed personal data have been collected in the Brazilian territory.

It also establishes that personal data collected in the Brazilian territory is understood as personal data whose data subject/owner is in the Brazilian territory at the time of the collection.

In a general way, the Brazilian Data Protection Law sets forth that the company will be regularly processing information from its employees, when: (i) fulfilling its obligations towards the employees, related to their employment agreements; (ii) fulfilling any obligations the employees and the employer may have, arising from the employment agreements of such employees; (iii) obligations under the scope of employment and business related activities; (iv) in defense of company's and employees' interests and rights; and (v) in the legitimate interests of the employer.

Further, LGPD expressly excludes from its protection (article 4) data originating from outside the Brazilian territory and which are not subject to communication, shared use of data with Brazilian processing agents, or subject to international transfer of data with other country than the country of origin, provided the country of origin provides personal data protection consistent with the provisions of this Law.

Therefore, whenever personal data is collected in a different country that does not have a regulation in force, and the information is shared with a processing agent in Brazil, it shall be subject to Brazilian LGPD.

In summary, the Brazilian Law allows the treatment of personal data collected without consent (regarded that an "acknowledgement" is given) in the following cases:

a) for compliance with a legal or regulatory obligation by the controller (employer in this case);

b) for the execution of contract or preliminary procedures related to a contract of which the data subject is a party;

c) to serve the legitimate interests of the controller (employer) or third party, except in the event that the rights and fundamental freedoms of the data subject prevail;

d) for the regular exercise of rights in judicial, administrative or arbitration proceedings;

e) when personal data becomes manifestly public, without losses to the rights of the data subject being protected.

The above mentioned “acknowledgement” may be given by updating company’s privacy and data protection policies that must be shared with the employees, as well as through training on such policies, etc.

Please note that whenever the consent of the data subject/owner for processing the information is required by law, or simply required for caution, LGPD sets forth that it is necessary to offer the means for the data subject/owner to easily revoke the consent granted, and in the event of change in the reason the data has been acquired, a new consent must be obtained from the data subject/owner.

In relation to the restrictions to share employee data across, whenever personal data is collected in a different country that does not have a regulation in force, and the information is shared with a processing agent in Brazil, it shall be subject to Brazilian LGPD.

In addition, personal data collected in Brazil will be subject to the LGPD, even if transferred abroad, and may be shared if the requirements for processing such data are met.

3.2. Chile

In Chile, personal data protection has been regulated by law since 1999, particularly under Personal Data Protection Law No. 19,628, which establishes general provisions regarding personal data processed by third parties. The main obligation falling to these parties is that they must inform data subjects of the purpose for which their data will be stored, inform of the possible public communication of the data and secure their written consent, although the law does not stipulate more specific formal requirements. Weaknesses in the law include the lack of adequate supervisory mechanisms and failure to cover the processing of information through digital media. To remedy these shortfalls, Chilean lawmakers have been working on a reform of the law for several years, proposing the creation of a personal data protection agency to ensure compliance with legal obligations and to penalize any breach thereof. This reform is in an advanced stage of its passage.

Data protection rights have been recently incorporated as a constitutional guarantee in the National Constitution.

Finally, in Chile there are no special restrictions when sharing employee data across borders. However, article 154 bis of the Labor Code very broadly provides that the employer must protect employee's personal data. This obligation applies to any information obtained as a consequence of an employment relationship. There are no other special restrictions or regulations in local law. The Chilean Employment Authority has ruled that this obligation does not allow the transfer of personal data between domestic entities within the country. Thus, this interpretation could be extended also to cross border employee data sharing.

3.3. Colombia

Colombian Decree No 1074 of 2015 has compiled the contents of all regulatory decrees governing data protection (including Decree 1377 of 2013 and Decree 886 of 2014). Said decree was recently modified by Decree 090 of 2018, which specified what subjects are obligated to register their databases before the Superintendence of Industry and Trade ("SIC"), which is Colombia's data protection authority.

Data controllers can transfer data across borders, according to Colombian data protection regulation; it could opt for one of the following options:

1) Previous and express consent. The consent should specify (i) who will control and process the personal data, (ii) what are the controllers' and the processors' contact details, (iii) how the data will be processed, (iv) what are the purposes of such a processing, (v) the rights data subjects are entitled to, and (vi) where they can find the privacy policy.

2) Data transfer agreement. Such an agreement should comply with the following requirements:

- Specify the purpose of the data transmission, that is, what is the scope of the processing and the activities that the developer will perform on behalf of YT for the treatment of personal data (see Concept SIC 16-193393).

- Stipulate that the data processor should safeguard the security of the databases in which personal data are contained. This requirement will only be met when security measures appropriate to minimize security risks.

- Include a confidentiality agreement.

- If data is to be transferred to another controller (as opposed to a data processor), Colombian law states that it could only be sent to countries with appropriate data protection standards. SIC has issued a list of countries that meet minimum privacy standards, where data could be transferred to.

3.4. Peru

Since 2011, Peru has specific personal data protection regulations in place. Law 29733 and its implementing regulations approved through Supreme Decree 003-

2013-JUS establish the regulatory framework for personal data processing rights and obligations, through two main pillars: protection and safeguarding of the appropriate exercise of rights by data subjects and compliance with the obligations falling to companies processing personal data. In September 2017, a legislative reform was approved, setting out a new classification for breaches and infringements of data protection regulations.

Compliance with personal data protection legislation is still rather incipient (which is why Peru is reforming the law specifically to include a sanctioning regime). The new rights and obligations established in the GDPR will require specific guarantees and measures that, in many cases, have not yet been seen in Peruvian legislation.

There are restrictions in Peru to share employee data across borders. In this sense, data subject consent is required. The employer has the obligation to inform the employers about the transfer of data to be performed. Also, cross border flows of data must be communicated with the Peruvian Data Privacy Authority. If the employer does not require the consent of the employee, this will constitute a serious infraction. If the employer does not communicate the cross-border flow of information to the authority, it will constitute a minor infraction.

The non-compliance of these regulations will be subject to economic fines. The range of the economic fine are (i) within US$ 630 to US$6,290 for minor infractions, (ii) within US$ 6,290 to US$ 62,880 for serious infractions; and (iii) within US$ 62,880 to US$125,000 for very serious infractions.

4. Employer – Employee Relationship in Argentina

4.1 Restrictions on Monitoring Employees

Argentine law requires that the employees be informed about the potential monitoring of corporate e-mails. Case law related to employee e-mail monitoring has established the validity of this procedure if: (i) the employee has been notified (and expressly accepted) the privacy policy of the company that enables the employer to monitor corporate email accounts, and (ii) only the corporate mail (not personal e-mail) can be monitored.

The lack of written or verbal instructions related to the use of internet communications in the company may create an expectation of privacy in the employee. Therefore, even when the employee agreed that the company is able to check corporate e-mails, if there is no provision in connection with the use of the company's e-mail for exclusively labour purposes, then the employee may object to the faculty of the employer based on an expectation of privacy.

If the employee consents to a specific search of his/her corporate e-mail, the evidence obtained to prove his misconduct is valid and can be used to sustain a dismissal with cause. There are several cases where e-mails have been used as evidence against employees without any questioning from the Court or defendants.

If the company is willing to prosecute criminal actions against the employee and the evidence of the crime needs to be obtained from the corporate e-mail account then the company will need a judicial order to check, copy and submit these e-mails to the criminal courts. In this case the Privacy Policy, having been accepted by the employee, will not be enough. Evidence obtained without judge authorization is null and void.

After the enactment of the Computer Crimes Law in June 2008 (Law 26,388), the "improper" access, opening, interception or publication of an electronic mail is a crime. "Improper" is an element of the crime that requires that the action be committed "against the law" or "without authorization".

4.2. Employees Data Access

In accordance with the DPA, any employee, as data subject, has the right to obtain from the employer all the personal data related to the subject and claim for the rectification, actualization or cancelation of her or his own data. Moreover, under the Constitution, any person shall have the right to file an action to obtain any personal data, contained in public or private records, and in case of falsehood or discrimination demand the suppression, correction, anonymization or updating of the record.

4.3. Sharing Employee Data with Third Party Service Providers

There are no restrictions other than the general restrictions set forth in the DPA as explained above, in other words, the personal data processed may be assigned only to fulfil the purposes directly related to the legitimate interest of the transferor and transferee with the prior consent of the data subject, which must be told about the purpose of the transfer and given the identity of the assignee or the tools with which he/she will be able to find that information out. The data subject consent is revocable and the transferor and the transferee are jointly liable vis-à-vis the data subject.

4.4. Restrictions on Transferring Data Overseas

There are no restrictions other than the general restrictions set forth in the DPA as explained above, in other words, the personal data processed may be assigned only to fulfil the purposes directly related to the legitimate interest of the transferor and transferee with the prior consent of the data subject, which must be told about the purpose of the transfer and given the identity of the assignee or the tools with which he/she will be able to find that information out. The data subject consent is revocable and the transferor and the transferee are jointly liable vis-à-vis the data subject.

5. Employee Privacy and Transactions

According to the DPA, the transfer of any type of personal information to countries or international or supranational entities which do not provide adequate levels of protection, is prohibited. The exception to this prohibition is to sign an international data transfer agreement that should contain rules of data protection (such as security measures or confidentiality) or to obtain the consent of the data subject.

The Rule 60 - E/2016 of the Data Protection Agency of Argentina, published in the Official Gazette on November 18, 2016, set forth aspects concerning the international transfer of personal data. Pursuant to the PDPL, the transfer of personal data to countries that have not enacted adequate legislation on personal data protection is forbidden. Rule 60 lists the countries with an adequate protection, similar to those recognized by the EU.

Furthermore, this Rule approved two sets of standard model clauses for data controller-data controller transfers as well as data controller-data processor transfers. Both model clauses were based on the EU Model Contracts for the transfer of personal data to third countries approved by Decision 2001/497/EC and 2010/87/EU.

Key Concepts and Principles of Employee-Related Data Protection Regulation in USA and the EU

Erica Schohn
Skadden, Arps, Slate, Meagher & Flom LLP
New York

I. United States

1. Employee Privacy in the United States

1.1. Privacy rules to protect employees' data in the US

In the US, there is no single, comprehensive national law governing the collection and use of personal data. Instead, there is a patchwork of federal and state laws that sometimes overlap, and most of which are directed toward protecting consumers and not employees.

Generally, federal statutes such as the Electronic Communication Privacy Act and the Computer Fraud Abuse Act protect electronic communications and electronic information.

The American with Disabilities Act ("ADA") and Family and Medical Leave Act ("FMLA"), as well as the Health Insurance Portability and Accountability Act ("HIPAA"), and similar state disability discrimination and leave statutes, protect employees' medical information.

Many states have data protection laws, which restrict or prohibit dissemination of "personal identifying information," such as an individual's social security number.

Some states (such as Arkansas, California, Colorado, Montana, New Hampshire, New Jersey, New Mexico and Oklahoma) have laws which prohibit employers from requiring, requesting, suggesting or causing a current or prospective employee from disclosing their social media usernames or passwords.

Some employers conduct consumer credit checks or background checks in connection with hiring or during the course of employment. These checks are governed, at the federal level, by the Fair Credit Reporting Act ("FCRA"). Many states also have laws which restrict or prohibit an employer's ability to obtain background checks and/or credit checks. The information received is generally considered sensitive data.

Certain states, such as California, also recognize a general right to privacy – which protects salary and other individualized personal information – however, such right to privacy is not absolute.

1.2. Penalty for breaching privacy rules.

The patchwork of statutes in the US means a variety of penalties for violating the various statutes, depending on the type of violation. Penalties may include civil penalties, such as fines and criminal penalties, such as imprisonment.

1.3. Restrictions on keeping employee records.

Generally, there is no statutory prohibition on an employer keeping employee records. Depending on the type of information being kept, however, employers may be subject to certain confidentiality and notice requirements.

The ADA and the FMLA, as well as similar state disability discrimination and leave statutes, require that any information obtained by an employer regarding the medical condition or history of an applicant or employee must be (i) collected and maintained on separate forms, (ii) kept in separate files, and (iii) treated in a confidential manner. Under HIPAA, health insurers and providers are required to implement technical, physical and administrative safeguards for protected health information in electronic form.

Within the last several years, many states, including California and New York, have enacted legislation requiring businesses maintaining computerized data that includes the owner's personal information to notify the owner of unauthorized access.

Some states have laws regarding the maintenance and destruction of information employers receive through background checks. For example, Massachusetts requires employers to: (i) store hard copies of criminal records in locked and secured locations (and for no longer than 7 years after an employee's employment ends); (ii) store electronic records using password protection and encryption; (iii) limit aces; and (iv) shred or destroy hard copies and delete electronic copies from hard drives and any backup systems.

1.4. Restrictions on monitoring employees in the US

Generally, there are no federal restrictions on employee monitoring. Courts addressing the issue weigh an employee's "reasonable expectation of privacy" with an employer's business justification for monitoring. Courts have largely held that an employer may engage in employee monitoring. However, it is considered best business practice for an employer to inform its employees they are subject to monitoring in the workplace or while using work-related devices. Some states might also require employee notice and/or consent of an employer's electronic monitoring of the employee's work or other activities.

Section 7 of the National Labour Relations Act prohibits employers from interfering with or restraining employees against exercising their right to engage in concerted activities for the purpose of collective bargaining. Accordingly, an employer's monitoring of an employee's social media use (and related policies) must account for the rights of workers to use social media to engage in concerted activities (such as organizing, picketing, and striking). Accordingly, employee policies and practices regarding monitoring should be narrowly tailored to serve legitimate business

interests, and not to prohibit or limit employees from engaging in concerted activities under the NLRA.

Some federal courts have applied the Electronic Communication Privacy Act (ECPA) and two of its subsections, the Stored Communications Act (SCA) and the Wiretap Act, which generally prohibits unauthorized access of stored electronic communications and unauthorized access of electronic information while the information is in transit, to employers who access employees' personal emails.

1.5. Rules that apply to employee's access to data held about them.

There is no federal law requiring employers to give employees access to their personnel file. However, some states give employees the right to review their personnel file in connection with a grievance, litigation, and/or performance review, subject to certain limitations.

If an employer takes an adverse employment action against a current or prospective employee in connection with a consumer credit report, the FCRA requires that the employer first provide the current or prospective employee with a copy of such report. Additionally, under state laws, an employee may be entitled to review a copy of the background check an employer performed on the employee. This is particularly the case when an employer takes an adverse employment action in connection with the information that the employer obtains.

1.6. Sharing employee data with third party service providers

Under the ADA, FMLA, and HIPAA, an employee's medical information may only be disclosed to (1) supervisors and managers who need to be informed regarding necessary work restrictions and necessary accommodations; (2) first-aid and safety personnel who need to be informed about emergency treatment; and (3) government officials who are investigating compliance-related issues. Information may also be released for purposes mandated by local, state or federal law.

1.7. Restrictions on transferring data overseas.

There are no federal statutes addressing data transfer of employee information overseas.

2. Employee Privacy and Transactions

2.1. Sharing employee data with a potential buyer before a transaction is signed.

Generally, employee data may be shared by an employer with a potential purchaser of the business. However, due to employee privacy concerns in states such as California, and recent state legislation banning the use of prior salary information in hiring practices, it is considered best practice not to disclose the names of employees tied directly to compensation information prior to signing. There are no specific statutory prohibitions on sharing employee data in a mergers and

acquisitions context. However, as noted, the previously discussed limitations on disclosing medical information and personal, identifying information apply.

Generally, there are no specific statutory prohibitions on disclosing employee information in the context of a transaction. However, employers should be aware of limiting disclosure of employees' private and confidential information, especially information relating to medical information, salary and personal, identifying information.

Finally, in the US there are no specific restrictions on transferring employee data when a sale is complete. However, under the Occupational Safety and Health Act, certain workplace safety information must be transferred to a successor employer.

II. France

1. Employee Privacy in France

1.1. Privacy rules to protect employees' data in the France.

French privacy rules are extensive and are included in a number of legal sources, such as:

- The 1978 Law on Computing, Files and Liberties (the "1978 Law") implemented the EU Directive 95/46/EC (the "Directive") on the protection of individuals.

- The 1978 Law was amended on December 2017 and May 2018 following the adoption of the General Data Protection Regulation ("GDPR") by the European Parliament on 16 April 2016.

- The GDPR entered into force on 25 May 2018 in the EU

- The law n° 2018-493, incorporating GDPR provisions in national law was promulgated on 20 June 2018 after a constitutionality check took place on 12 June 2018

- The transposition of the GDPR in France additionally required an implementation decree that was issued on 1 August 2018 (Decree n° 2018-687) and took effect on 4 August 2018

- The right to privacy enshrined in Article 9 of the French Civil Code;

- Various criminal law provisions of the French Criminal Code;

- The French Data Protection Authority guidelines ("Commission Nationale Informatique et Libertés*", or "CNIL") which have no legal value but help businesses to implement appropriate measures to protect personal data;

- The Article 29 Working Party's opinion on Data Processing at Work further clarifies that employees' consent is highly unlikely to be a legal basis for data processing at work, and employers must rely on another legal ground in most cases of employees' data processing

*The French Data Protection Authority (CNIL) is the independent administrative authority charged with supervising compliance with the law. It can conduct investigations and impose financial sanctions in case of breach.

French privacy rules and authorities give almost the same definition of personal data. According to the 1978 Law and the Directive, the GDPR does not bring major changes and defines personal data as "**any information relating to an identified or identifiable natural person** ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person" (Article 4).

It also distinguishes between ordinary and sensitive data.

Sensitive data is defined under Article 9 of the GDPR as "*data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited*".

Data that cannot be assigned to an individual, such as data provided by anonymized or pseudonym zed staff lists are not regarded as personal data in the sense of the GDPR.

The CNIL has already mentioned that "personal data are any anonymous data that can be double checked to identify a specific individual (e.g. fingerprints, DNA, or information such as "the son of the doctor living at 11 Belleville St. in Montpellier does not perform well at school")."

1.2. Penalty for breaching privacy rules in France.

Breach of employee privacy rights can be sanctioned as a criminal offence with a fine or even imprisonment sentence. The GDPR has attracted media and business interest because of the increased administrative fines for non-compliance.

The principle of secrecy of correspondence has constitutional value in France, linked to the right to privacy, it is thus punishable by a prison sentence of up to 1 year and a fine up to a €45,000 (French Criminal Code Art 226-15 and 432-9). Examples of fines imposed by the CNIL are as follows:

- In 2014, the CNIL fined **Google** €150,000 for the failure of its privacy policy to comply with the law. In this case, "The company does not sufficiently inform its users of the conditions in which their personal data was processed, nor of the purposes for processing. They may therefore neither understand the purposes for which their data are collected, which are not specific as the law requires, nor the ambit of the data collected through the different services concerned".

- In 2017, the Restricted Committee of the CNIL imposed a sanction of €150,000 against **Facebook Inc.** and **Facebook Ireland**. The Restricted Committee considered that these companies:
    - - "proceed to a compilation of all the information it has on account holders to display targeted advertising without having a legal basis".

    - -"do not provide direct information to internet users concerning their rights and the use that will be made of their data, in particular on registration forms;

    - -collect sensitive data of the users without obtaining their explicit consent. Indeed, no specific information on the sensitive nature of the data is provided to users when they complete their profiles with such data".

Under the GDPR, the administrative fines are discretionary rather than mandatory and must be imposed on a case-by-case basis. Administrative fines have to be "effective, proportionate and dissuasive". There are two tiers of administrative fines that can be levied: 1) Up to €10 million, or 2% annual global turnover – whichever is higher. 2) Up to €20 million, or 4% annual global turnover – whichever is higher. The fines are based on the specific articles of the Regulation that the organisation has breached. Infringements of the organisation's obligations, including data security breaches, will be subject to the lower tier, whereas infringements of an individual's privacy rights will be subject to the higher tier. When deciding whether to impose a fine and the tier, the CNIL must consider (Art. 83):

- The nature, gravity and duration of the infringement;
- The intentional or negligent character of the infringement;
- Any action taken by the organisation to mitigate the damage suffered by individuals;
- Technical and organisational measures that have been implemented by the organisation;
- Any previous infringements by the organisation or data processor;
- The degree of cooperation with the regulator to remedy the infringement;
- The types of personal data involved;
- The way the regulator found out about the infringement;
- The manner in which the infringement became known to the supervisory authority, in particular whether and to what extent the organisation notified the authority of the infringement;
- Whether, and, if so, to what extent, the controller or processor notified the authority of infringement; and
- Adherence to approved codes of conduct or certification schemes. The GDPR also gives individuals the right to compensation of any material and/or non-material damages resulting from an infringement of the GDPR. In certain cases, not-for-profit bodies can bring representative action on behalf of

individuals. This opens the door for mass claims in cases of large-scale infringements.

1.3. Restrictions for keeping employee records.

Employees' data collection and storage is tightly regulated by the law:

- data relating to an employee need only to be collected for proficiency check, administrative management, work organisation or social action;
- sensitive data should not be collected or held (employee's race, ethnicity, health, political or religious opinions or trade union membership);
- access to employee records is limited to those persons who are involved in human resources management;
- superiors can only have access to data required to perform their duties (i.e.: evaluation sheet, pay . . .);
- the employer has to take all measures to guarantee that data is safely stored and inaccessible to anyone without authorization;
- data relating to an employee may only be kept as long as the employee remains at the company and data such as payslips are kept for a maximum of 5 years from the data subject's departure.

1.4. Restrictions on monitoring employees in France

Monitoring of employees is heavily restricted in France. In fact, it shall not affect the rights and freedom of employees. Employees should be made aware that they are being or might be monitored, and the monitoring should be only for specified purposes and proportionate to those purposes.

- It is a specific criminal offence for an employer to read an employee's private correspondence, including e-mails marked "personal". According to the French Criminal Code this is a violation of the secrecy of correspondence (Article 226-15).
- An employer must not listen to employees' conversations without their knowledge. This is a disloyal behaviour (Cass. soc., 16 December 2017, n° 16-19.609).
- An employer who uses an employee's business phone to check the Facebook profile of another is responsible for intrusion on that employee's privacy.

As a result, an employer cannot submit a personal e-mail sent from a work computer as a piece of evidence before a judge (Cass. soc., 5 July 2011, n° 10-17.284).

CCTV monitoring

- Using CCTV to monitor the workplace is strictly regulated.
- The law does not allow employers to monitor employees at their workplace (i.e. staff room, toilets . . .).
- Only qualified staff can review videos.
- Videos must not be kept for more than one month.

- Installation of CCTV cameras in the workplace must be declared to the CNIL and if they cover any public space, they must be authorized by the local authorities (*préfecture de département*).
- Employee representatives must be informed and consulted before installation of CCTV cameras at workplace.
- Public and employees must be informed of the presence of CCTV cameras.

1.5. Employees' access to the data held about them.

Employees have access to their personal records and all data held by the employer about them (e.g. relating to recruitment, career history, annual review, pay, disciplinary matters) whether in paper or electronic form:

- Employees cannot access provisional or projected data about them (e.g. projected career progression) unless that information has been used to make an existing decision about a pay rise, promotion etc. Nevertheless, employees can access all HR data which has been used to reach a decision about them. (Articles 13, 22)
- The employer has the right to refuse a request for access to personal data if it appears manifestly abusive. (Article 23)
- The employer must allow employees their right to ask the data controller to rectify, complete, update, block or delete personal data that are inaccurate, incomplete, equivocal, expired or whose collection, usage, disclosure or retention is prohibited. (Article 16)

1.6. Sharing employee data with third party service providers

The CNIL advises employers to take all necessary steps to ensure security of data. There must be a legitimate purpose for the transfer, processing and archiving of the data by a third party supplier. Data itself must be adequate, relevant and not excessive for the purpose of the processing that is being outsourced.

The GDPR requires employers to take notice of the ways in which they process employee data, the purposes for which they process employee data and procedures in place for the collecting, transferring and storing of employee data. Employers will have to provide this information to each employee concerned about the sharing (Article 38, 1978 Law)

Moreover, in order to validly share employee data the employer will need to show this employee has given his/her consent to the processing. This consent must be freely given. (Article 7)

Article 35 of the 1978 law defines more precisely the role of a subcontractor. It states that its attitude towards the data should be bound by the instructions provided by the employer who is responsible for the treatment in the first place. As a third party, the subcontractor is liable for his contractual obligations of security and confidentiality aiming at protecting the personal data of employees against accidental or illicit destruction, alteration, diffusion or unauthorized access.

1.7. Restrictions on transferring data overseas.

Because of the presumption that employee data will not be adequately protected outside the EU, there are many restrictions on transferring data overseas.

Indeed, Art. 68 of the 1978 Law prevents the transfer of personal data to any foreign country with data protection provisions that are not at least equivalent to those in place within the EU [outside the EU the following countries listed by the EU Commission are deemed to have adequate safeguards in place: Andorra, Argentina, Canada, Faroe Islands, Guernsey, Iceland, Isle of Man, Israel, Jersey, Switzerland, Liechtenstein, New Zealand, Norway and Uruguay] except in certain cases including the following:

- EU model contractual clauses or binding corporate rules (BCRs) covering the parties to the transfer;

- The EU-US "Privacy Shield" (which replaces the previous "Safe Harbor" since August 2016) that allows companies to comply with data protection requirements when transferring personal data from the EU and Switzerland to the United States in certain circumstances including the case where the transfer is necessary to protect a person's life or public interest;

- By decision of the CNIL or by a decree of the French Administrative Supreme Court (Article 69)

In any case, it is mandatory to obtain the **prior, free, informed and express consent of the data subject to the transfer**. (Articles 7 and 8)

There will be no significant change with the GDPR and the adequacy decisions taken under the Directive will remain valid within the GDPR. Transfers of personal data to third countries outside the EU are only permitted where the conditions set by the GDPR are met (Article 44):

- Transfers to third countries, territories or specified sectors or an international organisation that the Commission has decided ensures an adequate level of protection do not require any specific authorization (Article 45(1)).
  Transfers are permitted where appropriate safeguards have been provided by the controller or processor and on the condition that enforceable data subject rights and effective legal remedies for the data subject are available. (Article 46)

The GDPR also includes under Article 49 a list of exemptions similar to those included in the Directive permitting transfers where:

- Explicit informed consent has been obtained;

- The transfer is necessary for the performance of a contract or the implementation of pre-contractual measures;

- The transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person; for important reasons of public interest; for the establishment, exercise or defence of legal claims; or in order to protect the vital interests of the data subject where consent cannot be obtained;

- The transfer is made from a register which according to EU or Member State law is intended to provide information to the public, subject to certain conditions.

GDPR also introduces two ways to justify international transfers (Article 46(2)):

- Data controllers (i.e. any person, public authority, department or any other organisation that determines the purposes and the means of the data processing) or data processors (i.e. a person processing personal data on behalf of the data controller) may rely on a code of conduct approved by the CNIL;

Data controllers may rely on a certification mechanism approved by the CNIL.

2. Employee Privacy and Transactions

2.1. Sharing employee data with a potential buyer before a transaction is signed.

One can take the view that employee personal data can be shared in the context of a due diligence without requesting permission of each employee as such disclosure is likely to be covered by the 'legitimate interest' justification under of the 1978 Law (Article 7(5°)).

Article 7 of the law of 20 June 2018 specifies that the processing of personal data must have received the consent of the data subject or must meet one of the following conditions:

1° compliance with any legal obligation to which the data controller is subject;

2° the protection of the data subject's life;

3° the performance of a public service mission entrusted to the data controller or the data recipient;

4° the performance of either a contract to which the data subject is a party or steps taken at the request of the data subject prior to entering into a contract;

5° the pursuit of the data controller's or the data recipient's legitimate interest, provided this is not incompatible with the interests or the fundamental rights and liberties of the data subject.

The general rules of adequacy, relevance and proportionality apply. Any information that is not necessary for the purpose of valuing the business / reviewing potential legal liabilities cannot be disclosed. In addition, restrictions such as these relating to disclose of sensitive personal information or transfers outside the EEC will apply.

In any case, the legitimate interest justification should be regarded as an exception to the rule and information should only be disclosed on a need-to-know basis and redacted in such a way that employees may not be identified.

2.2. Disclosing employee data in France in the context of a transaction

Essential employee information, in particular salary information and employment contracts, is generally disclosed for the bidder's advisers to review. In practice, sellers disclose large amounts of information which is not anonymized or in such a way that the individual is still identifiable.

To our knowledge, the CNIL has not issued any specific guidelines, but the usual rules on processing will apply to pre-transaction data sharing. In particular, data shared must be adequate, relevant and not excessive for the purpose of a transaction (e.g. wholesale disclosure of all employee data would be excessive). Sensitive personal data may not be shared and data may not be transferred outside of the EU except in the circumstances set out above.

Finally, there are no restrictions in France on transferring employee data when a sale is complete, since the buyer has a legitimate interest to receive all relevant employment data.

III. Germany

1. Employee Privacy in Germany

1.1. Privacy rules that protect employee data in Germany

As from May 25, 2018 the EU-DSGVO (EU-Directive 2016/679) came into force in all EU-Memberstates including Germany. Since the EU-DSGVO leaves room for some national regulations, a new version of the Federal Data Protection Act (Bundesdatenschutzgesetz - "BDSG"), will also come into force on the same day.

The regulation with priority is the EU-DSGVO which is "amended" by the BDSG.

Pursuant to Section 26 of the BDSG, the collection, processing (including a transfer or disclosure) and use of personal data is permissible if this is required

(i) to determine whether an employment relationship shall be established

(ii) to administer or terminate the employment relationship

(iii) to implement works council agreements

(iv) to detect crimes in case of reasonable suspicion or

(iv) the employee has freely granted written consent

In principle, these rules also apply to the transfer/disclosure of personal data in the course of due diligence proceedings.

According to Art. 6 EU-DSGVO the processing and transfer of personal data within the same group of companies inside the EU is permitted if there is a legitimate interest in such transfer and the data subject, i.e. the employee, cannot claim an overwhelming interest.

The transfer of personal data to recipients in countries outside the EU is permitted only if, in addition to the general transfer conditions or the consent of the data subject, there is an adequate level of data protection in the recipient jurisdiction or if the respective data subject agrees with the data transfer. The US is not considered by the EU authorities to offer adequate protection, except if there are further data protection mechanisms in place, such as entering into a cross-border data protection contract with EU-approved provisions. The new Privacy Shield Convention, which replaced the Safe Harbor Treatment, allows US companies to obtain a certificate as confirmation of adequate data protection in which case a transfer of personal data to the US is allowed.

1.2. Private or sensitive personal employees' data in Germany

Personal data are defined in Art. 4 EU-DSGVO as "any information concerning the personal or material circumstances of an identified or identifiable natural person" Personal data is generally understood to include any data identifying an individual, such as a name, telephone number, photo or email. This includes personal data generated in the context of business activities.

Some personal data are defined under Art. 9 EU-DSGVO as particularly sensitive. These are data about the racial or ethnic origin, political opinions, religious or philosophical beliefs, union memberships, health and sexual activities. It should be noted that some legal authors do also regard the membership in a works council as "sensitive data" because this could indicate a membership in a union. Processing of sensitive data is prohibited except if, among other reasons, this is necessary to claim or fulfil rights and obligations under the employment contract.

Data that cannot be assigned to an individual, such as provided for by anonymized staff lists, are not regarded as personal data in the above sense.

1.3. Penalty for breaching privacy rules in Germany

Under the new EU-DSGVO the sanctions in case of violations of the EU-DSGVO or the BDSG have become significantly stricter. Penalties now can reach 20 Mio EUR or 4 % of the annual turnover of the company, whatever is higher.

Individuals may claim damages according to Art. 82 EU-DSGVO. The employer has the burden of proof that the use of data was correct.

Intentional or wrongful collection or transfer of personal data in the course of a professional activity can be sanctioned as a criminal offence with a fine or even imprisonment of up to three years and two years in case the data transfer was for the purpose of own financial benefit.

1.4. Restrictions on keeping employee records.

There are no explicit restrictions but the general principles outlined above should be observed: records should be maintained as long as legitimately justified; held securely and safely, used only for the purposes for which they are given, kept up-to-

date and any out of date information should be destroyed. Typically employee records should be kept no longer than 5 years from the termination of employment.

1.5. Restrictions on monitoring employees in Germany

In case the private use of electronic equipment for e-mails or internet use is NOT allowed by the employer, the employer is allowed to monitor use of electronic communication or other activities, provided this is in accordance with the BDSG: employees should be made aware that they are being or might be monitored and the monitoring should be only for specified purposes and proportionate to those purposes (for example reviewing relevant emails only and none marked “private”).

As soon as the employer allows the private use of such electronic equipment, it is debated whether or not further restrictions apply.

Covert monitoring is rarely allowed. However, if adequate safeguards are in place it may be permissible if there are reasonable grounds to suspect that a criminal offence is being committed or national security or life is in danger.

1.6. Rules that apply to employee’s access to data held about them.

Employees, as data subjects, have the right to be told by the employer whether, why, how and what personal data is being processed about them. They can also request copies of the data held about them.

Employees can always request to review their personal records.

1.7. Sharing employee data with third party service providers in Germany

As long as the data provider is located within the EU AND the data transfer is required in order to administer the employment contract (e.g. transferring data to a pay roll agency), this is no problem. Employers should notify employees if their personal data is to be shared with a third party.

Only relevant data should be shared for the purpose for which it is given (for example bank account details for payroll purposes).

1.8. Restrictions on transferring data overseas.

There is a presumption that employee data will not be adequately protected outside the EU. Employers therefore need to ensure that if data is transferred outside the EU the recipient has adequate safeguards in place OR that the employee explicitly consents to the transfer.

Outside the EU the following countries on the EU Commission list are deemed to have adequate safeguards in place: Andorra, Argentina, Canada, Faroe Islands, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland, Uruguay.

Adequate safeguards so far deemed to exist if a recipient in the US is “safe harbour registered” with the US Department of Commerce (this is self-certified). According to the above mentioned decision of the European Court of Justice this is no longer the case. As an alternative, the data transferring parties should enter into a standard

"model clause" agreement on terms prescribed by the EU Commission (this entails committing to abide by the European Data Protection Directive).

2. Employee Privacy and Transactions

2.1. Sharing employee data with a potential buyer before a transaction is signed.

As a rule, staff lists providing for various information with respect to the employees such as position, date of entry, gender, age, etc. are to be disclosed anonymized in order to avoid assigning the data to an individual, as in such case they are no longer "personal data". If it is not possible to hide the identity of a particular employee (for example the CEO), their data might be disclosed only when the transaction is well advanced and then only to a clean team of those who need to know about that person's terms (for example it would be excluded from the data room and shared only with the potential buyer's human resources and finance directors and legal and financial advisers).

The processing of personal data of the members of the management and other key employees and the possibility for the potential buyer to review such data is generally considered as a necessary measure in connection with an acquisition and therefore to be regarded as a legitimate interest to process such data.

2.2. Sharing employee data in the context of a transaction

In case of an asset deal, buyer and seller are both obliged to provide the affected employees with written information about the legal and factual impacts of the transfer of their employment to the buyer. This requires the seller to provide the buyer with certain employee data, such as names and addresses. This is justified also under the BDSG.

Employers can transfer employee records to the new employer but, again, both parties should ensure that the records transferred are consistent with the data protection principles (for example, out of date data or information that is no longer relevant should not be shared/should be removed from the file before it is transferred) .

If the new owner is overseas, the data should only be transferred outside the EU in accordance with the requirements set out above for transferring data overseas.

In general, anonymized data can be provided at any time. But full employee data may only be provided for key employees holding exceptional positions.

IV. UK

1. Employee Privacy in UK

1.1. Privacy rules to protect employees' data in the UK.

On 25 May 2018 the General Data Protection Regulation ("GDPR") came into force across the EU (including the UK), replacing the Data Protection Act 1998 (the "DPA 1998") and the European Data Protection Directive (95/46/EC). The GDPR is intended to create a uniform approach to data protection across the EU.

On 23 May 2018, the Data Protection Act 2018 ("DPA 2018") received Royal Assent. The DPA 2018 has been introduced so that the UK and EU regimes are aligned post-Brexit.

UK data protection legislation applies to "data controllers" who own and/or determine how data should be processed and for what purpose (for example an employer) and "data processers" who process data at the direction and on behalf of the data controller (for example a payroll provider)

The GDPR sets out 7 key principles for processing data which are enhanced by the DPA 2018. The requirements are that data should be: (1) processed fairly, lawfully and transparently; (2) obtained only for specified and lawful purposes (the data should not be processed for any other purpose unless an exemption applies); (3) adequate, relevant and not excessive for those purposes (under the GDPR this is described as "data minimisation"); (4) accurate and up-to-date; (5) kept in a form that identifies the data subject no longer than is necessary; (6) processed in accordance with the employee (data subject)'s rights under the DPA 2018/GDPR; and (7) held securely and protected from loss or damage (by using appropriate technical or organisational measures). In addition there is a requirement that data is not transferred outside the EEA unless adequate safeguards are in place.

The principles are broadly similar to the principles under the DPA 1998. The key changes are as follows:

- an extension of obligations to (and ability to enforce breaches of the GDPR) against data processers directly;

- the new accountability principle. This specifically requires compliance with the principles and having appropriate processes and records in place to demonstrate compliance;

- controllers and processers must process personal data in accordance with the principles set out above and:

    - keep a detailed written record of their processing activities;
    - cooperate with supervisory authorities (in the UK the ICO);
    - ensure security and the ability to restore access to personal data;
    - notify the supervisory authority and data subject of any personal data breach (within 72 hours of becoming aware of the breach);
    - appoint a data protection officer where it is a public body, carries out large scale, systematic data monitoring or processing of personal data or data relating to criminal offences or convictions;

        - introduce technical policies to ensure access to, encryption of and minimisation of personal data;

- additional rights for data subjects:

    - the provision of information (including the identity and contact details of the controller, why data is being processed, recipients of the personal data, transfer of data out of the EEA, how long data will be stored, the right to request access to personal data about them, the right to complain to the ICO);

    - the right to rectification of information held about the data subject without undue delay;

    - the right to be forgotten (ie the erasure of personal data) in certain circumstances;

    - data controllers must respond to subject access requests within 28 days (reduced from 40);

    - consent will provide a lawful basis for processing only where it is "freely given, specific, informed and unambiguous". This limits consent as a lawful basis of processing employee data (the presumption is that employee consent is rarely "freely given") so employers must focus on other lawful reasons for processing, namely contractual necessity, compliance with legal obligations, the vital interests of the data subject or another natural person and the processer/controller's "legitimate interests". If relying on a legitimate interest the employer should keep a written impact assessment to demonstrate that proper consideration has been given to the data subject's rights and freedoms and that they have been balanced properly against the employer's legitimate interest;

    - the GDPR has extra-territorial effect. It applies to data controllers and processers based outside the EU who offer goods or services to data subjects in the EU (whether or not payment is required) or monitor the behaviour of data subjects in the EU so far as that behaviour is in the EU.

"Personal data" is any data about an individual from which that individual can be identified. "Special category data" is personal data which the GDPR says is more sensitive, and so needs more protection. Special category data is broadly similar to the concept of sensitive personal data under the DPA 1998.

Additional protections apply to special category data which is data about racial or ethnic origin, political opinion, religious or philosophical beliefs, trade union membership, physical or mental health, concerning a person's sex life or sexual orientation and genetic or biometric data (where used for ID purposes).

Personal data relating to criminal offences and convictions is not considered special category data and there are separate and specific safeguards for this type of data under the GDPR.

There is an exhaustive list of conditions for processing special category data, including (but not limited to) the following:

- the data subject has given explicit consent to the processing of those personal data for one or more specified purposes

- processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or the data subject (in the field of employment and social security)

- processing relates to personal data which are manifestly made public by the data subject.

Additional conditions and safeguards are provided by the DPA 2018.

1.2. Penalty for breaching privacy rules.

The Information Commissioner is able to:

- Prosecute organisations that breach the GDPR;
- Impose a maximum potential fine of:
    - the greater of €10M or 2% of the data controller or processer's global group turnover for its preceding financial year, for breaches of organisational rules, breaches by a data processer, failing to keep records or to meet breach notification requirements; or
    - o the greater of €20M or 4% of the data controller's global group turnover for its preceding financial year, for breaches of the data protection principles, rights of data subjects, transfer of personal data outside the EEA without ensuring that adequate safeguards are in place, certain rules of the member state or non-compliance with an order of the supervisory body (in the UK this is the ICO).

  The ICO has confirmed that it intends to use fines as the sanction of last resort.
- Issue enforcement notices and undertakings (the organisation will rectify a breach);
- Audit data controllers (the employer);
- Order a controller or processor to provide information;
- Obtain access to premises and data;
- Issue warnings of likely infringement on data processers;
- Order data controllers and processers to comply with a data subject's request to enforce his or her rights;

- Impose a temporary or permanent limitation on processing;
- Order the suspension of data flows to recipients outside the EEA.

1.3. Restrictions on keeping employee records.

With limited exceptions data controllers (including employers who process employee data) must register with the ICO. There are three different tiers of fee and controllers are expected to pay between £40 and £2,900. The tier depends on factors including: how many members of staff there are; annual turnover; and if the data controller is a public authority or charity.

There are no explicit restrictions but the general principles outlined above should be observed: records should be held securely and safely; used only for the purposes for which they are given; kept up-to-date; and any out of date information should be destroyed. Typically employee records should be kept no longer than 6 years from the termination of employment (when the UK contractual limitation period expires).

Data processors should assess the lawful basis on which they process employee data and, if relying on a "legitimate interest", keep a written record of their assessment of that interest in light of the employee's right to privacy and under the GDPR.

1.4. Restrictions on monitoring employees in the UK

The Regulation of Investigatory Powers Act 2000 prohibits the interception of electronic communication.

Employers can, however, monitor use of electronic communication or other activities provided this is in accordance with the DPA 2018 and GDPR: employees should be made aware that they are being or might be monitored; the monitoring should be only for specified purposes and it should be proportionate to those purposes (for example reviewing relevant emails only and none marked "private").

Covert monitoring is rarely allowed. However, if adequate safeguards are in place, it may be permissible if there are reasonable grounds to suspect that a criminal offence is being committed or national security or life is in danger. The standard is very high and pursuant to the GDPR employers are advised to keep their assessment of the reason for this action.

1.5. Rules that apply to employee's access to data held about them.

Employees, as data subjects, have the right to be told by the employer whether, why, how and what personal data is being processed about them. They can also request copies of the data held about them. A request for this information is a "subject access request" and must be made in writing. Following May 2018 the payment of an administration fee of £10 is no longer required and the employer must respond to a subject access request within 28 days. This can be a significant burden but the ICO will entertain extensions if the employer has a good reason.

Data controllers should ensure that their agreements with their data processers enable them access to or require cooperation from the data processer to provide the data that they have within the required time frame.

Employers are expected to make a proportionate search of any "relevant filing systems" which can include manual records (like managers' notes) if held in an accessible form and electronic records (including email accounts).

Confidential references given by the current employer are excluded.

1.6. Sharing employee data with third party service providers

Employers should notify employees if their personal data is to be shared with a third party and ensure that adequate safeguards are in place to ensure that the third party also complies with the DPA and GDPR. Following the introduction of the GDPR employers are advised to enter into more formal and specific data transfer agreements.

Only relevant data should be shared for the purpose for which it is given (for example bank account details for payroll purposes).

1.7. Restrictions on transferring data overseas.

The GDPR restricts the transfer of personal data to countries outside the EEA, or international organisations. There is a presumption that employee data will not be adequately protected outside the European Economic Area (EEA). Employers therefore need to ensure that if data is transferred outside the EEA the recipient has adequate safeguards in place.

Outside the EEA the following countries on the EU Commission list are deemed to have adequate safeguards in place: Andorra, Argentina, Canada, Faroe Islands, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland, Uruguay. Adequacy talks are ongoing with South Korea. The adoption procedure of the adequacy decision concerning Japan was launched on 5 September 2018.

The EU Commission has made partial findings of adequacy about the USA. The adequacy finding is only for personal data transfers covered by the EU-US Privacy Shield framework. To transfer personal data to a US organisation under the Privacy Shield, the organisation must have a current certificate on the Privacy Shield List and the certification must cover the type of data that is the subject of the transfer. The Privacy Shield framework remains under scrutiny in the EU.

If there is no adequacy decision about the country or territory, it may be possible to make the transfer subject to appropriate safeguards, which are listed in the GDPR.

The most common appropriate safeguards are set out below:

- Binding Corporate Rules (BCRs) – this is an internal code of conduct operating within a multinational group, which applies to restricted transfers of personal data from the group's EEA entities to non-EEA group entities.

• Standard data protection clauses adopted by the EU Commission (also known as 'model clauses') – there are four sets which the EU Commission has adopted. They must be entered into by the data exporter (based in the EEA) and the importer (outside the EEA).The clauses contain contractual obligations on the data exporter and the data importer, and rights for the individuals whose personal data is transferred. Individuals can directly enforce those rights against the data importer and the data exporter. The EU Commission has indicated that their standard model clause agreements will be updated to reflect the GDPR but at the time of this note no updates have been published.

If a restricted transfer is not covered by an adequacy decision, nor an appropriate safeguard, the transfer may be possible if its covered by one of the exceptions set out in Article 49 of the GDPR.

Some of the exceptions are set out below:

- The individual (whose personal data is the subject of the transfer) has given his or her explicit consent to the restricted transfer.
- There is a contract with the individual and the restricted transfer is necessary to perform the contract. This exception can only be used for occasional restricted transfers.
- The restricted transfer is necessary for important reasons of public interest.
- The restricted transfer is required to establish, make or defend a legal claim

2. Employee Privacy and Transactions

2.1. Sharing employee data with a potential buyer before a transaction is signed.

It is generally considered that processing personal data in anticipation of a business or company sale is to promote the employer's legitimate interests and so is permissible. However, the employer should still comply with the data protection principles set out above (only relevant data should be disclosed and the employer should require the recipient to enter into an appropriate data transfer agreement including commitments regarding confidentiality and security).

It is rare that the employees' identities are relevant at this stage so many employers redact or anonymise the data so that individuals cannot be identified (if that is the case it is no longer "personal data").

Employee data is typically disclosed in phases as the transaction progresses and the information becomes more relevant: for example in the pre-bid phase only general and anonymous data would be disclosed. If it is not possible to hide the identity of a particular employee (for example the CEO) their data might be disclosed only when the transaction is well advanced and then only to a clean team of those who need to know about that person's terms (for example it would be excluded from the data room and shared only with the potential buyer's human resources and finance directors and legal and financial advisers).

2.2. Sharing employee data in the context of a transaction

Employers must disclose specified employee data at least 28 days before an asset transfer that falls within the Transfer of Undertakings (Protection of Employment) Regulations 2006 (TUPE). The ICO has acknowledged that the provision of this data is a legitimate obligation for the employer and that it should be provided, however, the employer and recipient should both comply with the data protection principles and GDPR as set out above.

Additional employee data that can be shared with a potential buyer after a transaction is signed but before it is closed.

In order to comply with the GDPR the seller should prepare an impact assessment and ensure that there is a legitimate interest in transferring the employee data to the buyer. The data that can be transferred will vary, dependent on the circumstances and the reason for the transfer but generally the seller will be able to share data that is necessary to enable the buyer to meet its obligations to the employees or under the purchase agreement (for example data that is necessary to establish payroll can be shared with the payroll provider and employees at the buyer who need to know this information to process pay but no one else). The seller should also consider whether any NDAs or confidentiality agreements between the parties to the transaction are adequate to protect this personal data and might want to make the transfer of employee data subject to a specific data transfer agreement.

Employers can transfer employee records to the new employer but, again, both parties should ensure that the records transferred are consistent with the data protection principles and GDPR (for example out of date data or information that is no longer relevant should not be shared/should be removed from the file before it is transferred).

If the new owner is overseas, the data should only be transferred outside the EEA in accordance with the requirements set out above for transferring data overseas.