GDPR IN AN EMPLOYMENT CONTEXT /

GDPR
IN AN EMPLOYMENT CONTEXT
/

CONTENT

AUSTRIA

1. As an EU Regulation, the GDPR is directly applicable and must not be implemented into national legislation. However, the GDPR includes certain articles that give Member States the opportunity to have specific national legislation in execution of the GDPR. This is, for instance, the case for the processing of employee personal data.

1. Has your country made use of this opportunity to have specific national rules regarding the processing of employee personal data? If so, please comment on these rules.

2. If not, has your country adopted other national data protection legislation in execution of the GDPR that could be relevant in an HR context? If so, please give a short bullet-point overview of the relevant provisions.

1. No, the Austrian legislator did not implement specific rules regarding the processing of employee data. However, the Austrian Data Protection Act *(Datenschutzgesetz, "DSG")* contains a few selective provisions in context with HR data (see in detail question 2).

2. Neither has the Austrian legislator adopted other national data protection legislation in execution of GDPR, which could be relevant in an HR context.

2. Does any other employment-related privacy legislation exist in your country (not necessarily in execution of the GDPR)? Has the GDPR impacted this existing privacy legislation?

DSG contains a few employment-related provisions. These provisions were substantially maintained after the implementation of GDPR:

- In section 6 DSG, the so-called "data secrecy" *(Datengeheimnis)* is regulated. This section provides that data controllers and their employees or quasi-employees have to keep data that they have access to or have been entrusted to in context with their work confidential.

- Section 12 para 4 no 2 DSG declares the processing of images (which covers photos and videos) for the purpose of monitoring/controlling employees unlawful.

/ Nino Tlapak
Attorney
+43 1 533 4795 23
nino.tlapak@dorda.at

- In case there is a work council implemented in a company, the council must, pursuant to section 91 para 2 of the Work Organisation Act *(Arbeitsverfassungsgesetz, "ArbVG")*, be upfront informed what types of personal employee data shall be processed by the company owner by automated means and what processing and transfers it provides for in general. Upon request, the works council shall be enabled to examine the basis for data processing and transmission. Unless the work council is entitled to an unlimited right of inspection according to section 89 ArbVG or other legal provisions (e.g. if the inspection is necessary for the work council to check the internal records of the company owner about the employees' remuneration or to revise the observance of labour law agreements), the consent of the individual employee is necessary to enable the work council to access the employee's personal data.

- The introduction of systems for the automated determination, processing and transmission of the employee's personal data by automatic means, which go beyond the determination of general identification data and professional requirements, requires prior consent of the works council according to section 96a para 1 no 1 ArbVG. In addition, any control system or measure that may allow the employer to control its employees requires prior consent by the works council.

- The original draft of the Austrian Implementation Act of GDPR contained a clause which declared the provisions of ArbVG that govern the processing of personal data provisions within the meaning of Art 88 GDPR. This clause was, however, removed in the legislative process. Nevertheless, the respective provisions of ArbVG are to be understood as employee data protection, whereas a violation of these provisions also leads to penalties according to Art 83 no 5 lit d GDPR.

- Besides, kindly note that the Austrian Data Protection Authority *(Datenschutzbehörde, "DSB")* is rather stringent as regards accepting legitimate interests of the employer to transfer employees' personal data, even within the same group of entities. Thus, there is persistent case law as regards whistleblowing hotlines, compliance management systems, CCTV and location data, which do often lead to national limitations.

3. The information obligation of employers (data controllers) towards their employees has been extended under the GDPR. Therefore, the current information clauses/policies will probably no longer be sufficient.

1. By what means (e.g. (an annex to) the employment contract, work rules, a policy) would you recommend employers in your country provide employees with this extended information?

2. Should any particular procedure be complied with?

1. We recommend a separate privacy policy for employees. Further, a specific privacy policy for job application procedures should be prepared, which is to be provided to applicants at the earliest possible date; at best, this policy should also be available and downloadable at the data controller's website.

2. A specific procedure, such as a signed confirmation of every employee that he has received the policy, is not mandatory.

3. In most cases, current employee contracts already contain a clause with regard to data secrecy. These clauses have to be re-assessed and usually adapted. In practice, we note that further to the information obligation, all processing of HR data must be assessed to be GDPR-compliant: e.g. as regards business mobile phones, private/business usage of devices, transfer of employee data within a group of companies, whistleblowing hotlines, CCTV etc.

4. Is 'consent of the employee' used as a legal justification ground to process his/her data in your country, required/advised/ discouraged? Can you illustrate with some examples?

Consent within the meaning of Art 4 no 11 GDPR is not discouraged as a legal justification in HR-context in general. However, in most cases, many data processings can be justified by other legal bases such as Art 6 para 1 lit b and lit c GDPR (in particular to fulfill labour and social law obligations, for the performance of employment contracts, and, as regards the processing of sensitive data, in order to exercise the rights conferred by labour, social security and social protection law and fulfill the respective duties).

Employee consent declarations are a useful legal basis for individual data processing such as the usage of photos of the employee for social media purposes or for the (proportionate) control of internet usage in case private usage is allowed. In any case, it must be ensured that the consent is declared voluntarily and can be granted separately from other contract declarations *(Koppelungsverbot)*. Consents may therefore continue to be useful in the case of processing operations carried out (also) for the benefit of the consenting employee.

The DSB usually requests information and evidence as regards employees' free will to provide their consent. Thus, a practicable alternative for employees' that (i) do not provide or (ii) revoke any given consent has to be implemented.

5. The GDPR provides that a DPO benefits from dismissal protection. However, the GDPR does not provide for any penalties for the employer in case of any violation of this dismissal protection.

Can an employer in your country be sanctioned for dismissing a DPO for reasons related to his/her tasks as DPO? If yes, on what basis and what will be the penalty/ies?

A dismissal protection for DPOs was not implemented in Austrian law. Further, Austrian law does also not provide for a penalty for employers; also, there is no established case law on this. A penalty for employers is therefore questionable in general.

However, a termination due to the employee's activities as DPO would be contestable as a "termination of employment for proscribed reasons/inadmissible motifs".

6. What legal action(s) can an employee take against an employer in your country if he/she believes that his/her data protection rights are not being respected?

Legal actions in HR-context do not differ from the actions open to everybody pursuant to GDPR and DSG. Employees may therefore lodge a complaint with the DSB.

7. Does your national legislation fix a storage period for HR-related documents?

Austrian legislation does not provide for particular storage periods, but rather provides for different limitation periods to assert claims that need to be considered when implementing storage/data deletion processes and limits, depending on the type of document and personal data contained. The periods must be assessed in detail and on a case-by-case basis, whereas this table may only give a brief overview:

- Dismissed job applicants may, pursuant to section 15 of the General Law on Equal Treatment *(Gleichbehandlungsgesetz, "GlBG")*, assert claims up to six months after rejection of their application.
- According to section 1486 of the Austrian Civil Code *(Allgemeines Bürgerliches Gesetzbuch, "ABGB")*, claims of employees for remuneration expire within 3 years. Accordingly, records on classification of employees, working hours, travel costs, premium or bonus agreements, etc. should be kept at least for the duration of the three-year limitation period.
- In context of social insurance and also tax law, a seven year retention period is mandatory (Section 132 of the Federal Fiscal Code, *Bundesabgabenordnung*).
- However, the employee's entitlement to demand the issuing of a recommendation letter only lapses after 30 years pursuant to Section 1479 ABGB. However, only general data on the employee and its employment need to be retained for this purpose.

8. The GDPR obliges each country's supervisory data protection authority to draw up a list of the kinds of processing operations that, in its view, require a Data Protection Impact Assessment ('DPIA'), i.e. the controller's assessment of the impact of the envisaged processing operations on the protection of personal data where a type of processing is likely to result in a high risk. The supervisory data protection authority may also (but is not obliged to) draw up a list of the kinds of processing operations for which no DPIA is required.

1. Has your country's supervisory data protection authority only established a list of processing operations that require a DPIA or also a list of processing operations that do not require a DPIA?

2. Do any of these lists include HR-related processing operations?

1. The Austrian DSB has issued both, a list of processing operations that require a DPIA as well as a list of processing operations that do not require a DPIA. Both documents were issued as a "regulation" *(Verordnung)* and may be accessed only in German language via the following link: https://www.dsb.gv.at/verordnungen-in-osterreich

2. Yes, the list of processing operations that do not require a DPIA contains "*Personalverwaltung*". In this context, the regulation specifies the following data processing activities (literal transcription):

   - Processing and maintaining records of personal data for salary, salary accounting purposes and compliance with recording, information and reporting obligations, in so far as required by law or "collective law" or contractual employment obligations;

   - Processing and maintaining records of personal data in context with their service law, remuneration, education or other relation to the employment relationship of public servants and other people remunerated by public authorities (e.g. also contract staff and temporary staff, members of parliament and officials) as well as volunteers and civilian servants (without remuneration) by the service authority and personnel offices for the purpose of individual personnel measures and statistical evaluations;

   - Processing and maintaining records of personal data of applicants, if such data have been provided by the data subject;

   - Processing of special categories of personal data within the meaning of Art 9 GDPR and processing of personal data on criminal convictions and offences within the meaning of Art 10 GDPR within the scope of this exception are only permitted on the basis of a legal authorisation or legal obligation.

3. In addition, the recently issued Black List distinguishes between processing operations where a DPIA must already be carried out in the case of one criterion and those where at least two different criteria must apply cumulatively in order to trigger this obligation. This is relevant, since a DPIA shall be carried out if at least two of the following criteria are met (while employees itself are mentioned):

   - Large-scale processing of special categories of personal data;

   - Large-scale processing of data on criminal convictions and offences;

   - Collection of location data as defined in the Austrian Telecommunications Act *(Telekommunikationsgesetz – TKG)*;

   - Processing of data on persons in need of higher protection (e.g. minors, employees, patients, mentally ill persons and asylum seekers);

   - Merging and/or comparing of data sets from several processing operations, provided that they are processed for purposes other than originally intended.

9. Has your country's supervisory data protection authority given any employment law-related advice or made any recommendations since the GDPR has entered into force?

No.

10. 1. Are there in your country any additional conditions, on top of what is provided for within the GDPR, to process any special categories of personal data? If so, which conditions and for which type(s) of data do they apply?

2. Does your national legislation authorize the processing of personal data relating to criminal convictions and offences? If so, when is this authorized and what are the appropriate safeguards that should be complied with (if any)?

1. Collective agreements, in practice mostly so-called *Betriebsvereinbarungen* closed between the works council and the employer, may allow the processing of special categories of data only if they provide for appropriate safeguards for the fundamental rights and interests of the data subjects. However, this requires a rigorous examination of the respective conditions and measures for data processing. These issues are not explicitly regulated in DSG, but result from the already pre-GDPR existing data protection-implications of labour law now in connection with GDPR. In addition, section 10 of an Austrian law amending the labour contract law *(Arbeitsvertragsrechts-Anpassungsgesetz,* "AVRAG") requires the consent of each individual employee for a compliant introduction and use of specific control measures and technical systems which could affect human dignity.

   Besides, a Health Telematic Act *(Gesundheitstelematikgesetz, "GTelG")* exists that provides for specific IT measures in the context of processing personal health data.

   However, further specific sections are scattered in Austrian law as they are contained in specific material laws, e.g. ruling data processings and transfers of insurances, doctors, healthcare providers etc.

2. Yes. Indeed, section 4 para 3 DSG provides that the processing of personal data concerning acts or omissions which are punishable by law or administrative authorities, in particular also concerning the suspicion of the commission of criminal offences, as well as concerning criminal convictions or preventive measures, is permissible in compliance with the provisions of the GDPR if there is (i) an express statutory authorization or obligation to process such data or (ii) if the permissibility of the processing of such data results from statutory duties or if the processing is carried out to safeguard the legitimate interests of the responsible person or a third party in accordance with Art 6 para 1 lit f GDPR and the manner in which the data processing is carried out ensures that the interests of the data subject are safeguarded in accordance with GDPR and DSG.

The Austrian legislator unfortunately refrained from describing or even demonstrating what kind of measures could constitute appropriate safeguards. According to the opinion of legal literature prior to GDPR, such data might be processed, if an evaluation of the respective interests shows that the interests of the data controller (employer) prevail. Examples include the processing of criminal records data for employees of a security service or a cash transport company, employees in the financial administration or those whose activities require the confidentiality of commercial and industrial secrets.

BEL GIUM

/ Philippe De Wulf
Partner
+32 (0) 2 426 14 14
philippe.dewulf@altius.com

1. As an EU Regulation, the GDPR is directly applicable and must not be implemented into national legislation. However, the GDPR includes certain articles that give Member States the opportunity to have specific national legislation in execution of the GDPR. This is, for instance, the case for the processing of employee personal data.

1. Has your country made use of this opportunity to have specific national rules regarding the processing of employee personal data? If so, please comment on these rules.

2. If not, has your country adopted other national data protection legislation in execution of the GDPR that could be relevant in an HR context? If so, please give a short bullet-point overview of the relevant provisions.

Belgium has not (yet) made use of the opportunity offered by the GDPR to have more specific national provisions on the processing of employee personal data in the employment context.

However, in execution of the GDPR, Belgium adopted a new general Data Protection Act on 30 July 2018, which entered into force on 5 September 2018. This Act does not include specific national provisions for the processing of employee data, but does include provisions that are general in scope, but could be relevant or could have an impact in an HR context, such as, for instance:

- For the processing of genetic, biometric and health data, the new Belgian Data Protection Act ('BDPA') determines a number of additional conditions (in addition to the GDPR) for processing such data (see question 10 below)

- For certain infringements of the data protection rules, the BDPA provides for – lower - criminal penalties, besides the huge administrative fines provided for by the GDPR; a company cannot receive both types of penalty for the same infringement.

2. Does any other employment-related privacy legislation exist in your country (not necessarily in execution of the GDPR)? Has the GDPR impacted this existing privacy legislation?

Yes, besides the GDPR, Belgium has specific employment-related privacy legislation that already existed prior to the GDPR entering into force, namely:

- A specific national Collective Bargaining Agreement (CBA n° 81) on the monitoring of electronic online communication data (internet & e-mail);

- A Belgian Act and CBA (CBA n° 68) on the use of camera surveillance;

- A national Collective Bargaining Agreement (CBA n° 89) on exit checks.

This legislation continues to apply following the GDPR's entry into force.

However, the Act on camera surveillance has recently undergone some changes, amongst other reasons, because of the GDPR.

Amongst other things, this Act now expressly provides that a record of image processing activities must be maintained, which includes a number of types of additional compulsory data in addition to the data that the GDPR requires to be registered in the processing activities' records.

In addition, the cameras must be declared to the police, by means of an online portal *www.aangiftecamera.be*. (It is no longer required to report such camera surveillance to the Data Protection Authority).

However, this Act on camera surveillance does not apply to the use of cameras on the work floor for purposes of safety and health, the protection of the company's goods, supervision of the production process or surveillance of employees. If the use of cameras is limited to these purposes, only the CBA n°68 applies. If not or if these cameras would also surveille a publicly-accessible place (such as a shop that monitors its customers, but also its employees), the company is obliged to comply with the Act.

3. The information obligation of employers (data controllers) towards their employees has been extended under the GDPR. Therefore, the current information clauses/policies will probably no longer be sufficient.

1. By what means (e.g. (an annex to) the employment contract, work rules, a policy) would you recommend employers in your country provide employees with this extended information?

2. Should any particular procedure be complied with?

The GDPR only requires that the information is given in writing and that it must be concise, transparent, intelligible and easily accessible, and use clear and plain language.

The GDPR does not state the required format or modality by which such information should be provided to the employees.

As a consequence, an employer can freely choose the means to inform its employees. This could be done by a specific data protection clause in the employment contract, an annex to such a contract, or in the work rules or in a written policy. However, given the fact that the employee should be notified about any significant changes to the information clause, we recommend opting for a medium that is easy to modify. Therefore a document, such as a policy, that is separate from the employment contract or the work rules is preferable.

The Working Party 29 (now called the European Data Protection Board or "EDPB") recommends making the privacy policy also freely-accessible online (such as through an intranet). To avoid 'information fatigue' and to increase the transparency of such a policy, the EDPB furthermore encourages a 'layered' structure. This allows a more user-friendly navigation to particular aspects of the policy and could also be used to highlight certain specific topics. In addition, the privacy policy must be clearly differentiated from other non-privacy related information.

Changes to a privacy policy must always be notified to the employees prior to the commencement of the processing by way of an appropriate modality. In general, an e-mail will be sufficient as this will notify the employees of such a change.

4. Is 'consent of the employee' used as a legal justification ground to process his/her data in your country, required/advised/discouraged? Can you illustrate with some examples?

In an employment context, consent can almost never be used as a valid processing ground. This is because consent should be given freely. However, as the European Data Protection Board ('EDPB') and the Belgian Data Protection Authority have stated on multiple occasions, due to the imbalance of power in an employment relationship, consent is seldom given freely by an employee. Moreover, the employee can always withdraw his or her consent.

In most processing activities related to an employment context, the appropriate legal ground is therefore the execution of the contract with the employee, a legal obligation or a legitimate interest of the employer.

Only in exceptional circumstances, consent could be a valid processing ground.

The BDPA has for example indicated that consent could be an appropriate legal basis for the processing of photos that are not strictly necessary (e.g. photos of social events, photos published on the company's website, etc.) and if the refusal would not give rise to any negative effects for the employee.

5. The GDPR provides that a DPO benefits from dismissal protection. However, the GDPR does not provide for any penalties for the employer in case of any violation of this dismissal protection.

Can an employer in your country be sanctioned for dismissing a DPO for reasons related to his/her tasks as DPO? If yes, on what basis and what will be the penalty/ies?

Indeed, neither the GDPR nor the Belgian Data Protection Act provide for any sanctions for the employer in the case of a DPO's dismissal for reasons related to his/her tasks as DPO. Until further provisions or case law clarifications are made, it seems that, in Belgium, the DPO could claim an indemnity based on a manifestly unreasonable dismissal or abuse of rights.

The indemnity for a manifestly unreasonable dismissal ranges from between 3 and 17 weeks of salary (on top of the normal indemnity in lieu of notice), but it is not excluded that higher indemnities would be granted on the basis of 'abuse of rights'.

6. What legal action(s) can an employee take against an employer in your country if he/she believes that his/her data protection rights are not being respected?

A data subject (e.g. an employee) has several ways to enforce his/her rights.

First, he/she could lodge a complaint with the Belgian Data Protection Authority, which, in contrast to the former Privacy Commission, has more far reaching powers. The BDPA could, amongst other things, conduct an investigation, question personnel and consult IT systems. It can also take corrective measures that include: issuing a warning, ordering a temporary or definitive limitation of the processing operations or imposing an administrative fine.

Second, a data subject (such as an employee) could seek an injunction with the President of the Court of First Instance. The Belgian Data Protection Act provides for a specific fast-track procedure for a data protection infringement that is similar to the procedure that existed under the previous regime (before the GDPR entered into force).

Third, a data subject could also claim for material or non-material damages with the courts.

We note that a data subject has the right to mandate a non-profit body, organisation or association to exercise such rights. However, such an organisation must meet certain criteria. Class actions for data protection infringements are not possible under the Belgian Data Protection Act.

7. Does your national legislation fix a storage period for HR-related documents?

Minimum legal retention period

Only for a limited number of employment-related documents is there a legal obligation to retain these documents for a certain time-period defined by law (often 5 years). This is, amongst other things, the case for the so-called 'social documents' (i.e. the personnel register, the individual accounts and pay slips, specific employment contracts such as contracts for students, temporary work or professional immersion contracts, cash for car addenda/agreements), obligatory documents for part-time workers, work accident declarations, all documents relating to the employment of foreign employees (work permit, Limosa, etc.), etc.

Recommended retention period

Under the GDPR, personal data may only be kept for "no longer than is necessary" and for the purposes for which the data has been collected/processed. However, keeping employment-related documents, which could serve the employer's case against possible claims from employees or authorities during a retention period based on the statute of limitations of such possible claims, is accepted.

8. The GDPR obliges each country's supervisory data protection authority to draw up a list of the kinds of processing operations that, in its view, require a Data Protection Impact Assessment ('DPIA'), i.e. the controller's assessment of the impact of the envisaged processing operations on the protection of personal data where a type of processing is likely to result in a high risk. The supervisory data protection authority may also (but is not obliged to) draw up a list of the kinds of processing operations for which no DPIA is required.

1. Has your country's supervisory data protection authority only established a list of processing operations that require a DPIA or also a list of processing operations that do not require a DPIA?

2. Do any of these lists include HR-related processing operations?

The Belgian Data Protection Authority has established both a list of processing operations that require a DPIA and a list of processing operations that do not require a DPIA.

The list of processing operations that require a DPIA does not include processing operations that are directly related to HR matters. For some however, there could be a connection with HR-matters, e.g. for the use of devices connected to the internet to evaluate personal aspects of personnel (e.g. tracking devices).

The list of processing operations that do not require a DPIA includes a few HR-related processing operations, namely:

- The processing that only concerns the data necessary for the administration of the salaries of those individuals employed by or active on behalf of the controller;

- The processing that only concerns the administration of the staff employed by or active on behalf of the controller.

9. Has your country's supervisory data protection authority given any employment law-related advice or made any recommendations since the GDPR has entered into force?

Since the GDPR has entered into force, the Belgian Data Protection Authority has not given any specific advice or made any recommendations on employment law. However, the BDPA has given a few more general pieces of advice/recommendations that could be important in an HR-context, i.e. :

- Recommendation on DPIA's

- Recommendation on records of processing activities

- Recommendation on the appointment of a data protection officer

10.

1. Are there in your country any additional conditions, on top of what is provided for within the GDPR, to process any special categories of personal data? If so, which conditions and for which type(s) of data do they apply?

2. Does your national legislation authorize the processing of personal data relating to criminal convictions and offences? If so, when is this authorized and what are the appropriate safeguards that should be complied with (if any)?

1. **Additional conditions**
   For the processing of genetic, biometric and health data as well as for personal data relating to criminal convictions and offences, the new Belgian Data Protection Act ('BDPA') determines a number of additional conditions (on top of the GDPR) for processing such data. These additional conditions already existed on the basis of the 'old' Belgian Data Protection Act, which applied before the GDPR entered into force, and were confirmed in the new BDPA. These additional conditions are:

   - the obligation to keep a list of the categories of persons having access to the aforementioned type of data as well as a description of their role regarding the processing of such data;
   - such persons, who have access, should be bound by a statutory or contractual confidentiality obligation.

2. **Additional exceptions**
   The BDPA provides for a few, very limited exceptions to the prohibition on processing personal data relating to criminal convictions and offences (e.g. when this is necessary for the management of own disputes). Also the data subject's consent is provided for as a general exception, but this exception cannot be used by employers vis-à-vis their employees (as consent cannot be given freely in an employment context: see question 4 above). Therefore, in principle, employers will not be able to retain or to process the criminal record of an employee or an applicant (but the employer may ask to view a copy without processing it).

The appropriate safeguards are indicated above under point (1).

FRANCE

/ Patrick Thiébart
Partner
+33 (0)1 45 05 80 08
pthiebart@jeantet.fr

/ Olivier Angotti
Partner
+33 (0)1 45 05 81 78
oangotti@jeantet.fr

/ Déborah David
Partner
+33 (0)1 45 05 82 06
ddavid@jeantet.fr

1. As an EU Regulation, the GDPR is directly applicable and must not be implemented into national legislation. However, the GDPR includes certain articles that give Member States the opportunity to have specific national legislation in execution of the GDPR. This is, for instance, the case for the processing of employee personal data.

1. Has your country made use of this opportunity to have specific national rules regarding the processing of employee personal data? If so, please comment on these rules.

2. If not, has your country adopted other national data protection legislation in execution of the GDPR that could be relevant in an HR context? If so, please give a short bullet-point overview of the relevant provisions.

1. Specific national rules regarding the processing of employee's personal data in the employment context have not been implemented (yet) in France.

2. Nevertheless, France adopted a new general Data Protection Act No. 2018-493 on 20 June 2018 ("FDPA") which amended its former legislation (Data Protection Act No. 78-17 on 6 January 1978) in order to comply with the GDPR's provisions.

   The FDPA does include provision that are mainly general in scope. However, the FDPA includes some national provisions that could be relevant or could have an impact in an HR context.

   For instance:
   Article 8 of the FDPA indicates that processing biometric data for the purpose of uniquely identifying a natural person is prohibited. However, the FDPA determines additional conditions in addition to the GDPR for processing such data.

   Indeed, the processing of biometric data is allowed for employers and administrations when the processing is strictly necessary for the access's control to (i) the workplace and (ii) the work equipment and applications used in the context of the tasks entrusted to employees, agents, trainees or service providers.

2. Does any other employment-related privacy legislation exist in your country (not necessarily in execution of the GDPR)? Has the GDPR impacted this existing privacy legislation?

Yes

The French Labour Law provides specific requirements regarding employee's privacy (mainly through the French Labour Code and many case law) that cover the following employment-related topics: CCTV surveillance within the work premises, entry and exit check, monitoring of electronic online, communication data (the Internet and emails), telephone monitoring, geo-tracking ...

Such requirements continue to apply following the entry into force of the GDPR.

3. The information obligation of employers (data controllers) towards their employees has been extended under the GDPR. Therefore, the current information clauses/policies will probably no longer be sufficient.

1. By what means (e.g. (an annex to) the employment contract, work rules, a policy) would you recommend employers in your country provide employees with this extended information?

2. Should any particular procedure be complied with?

1. Under French Law, employer must inform each employee individually prior to the collect of their personal data according to Article L1222-4 of the French Labour Code.

   Article 12 of the GDPR only sets forth that the information is provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language. However, the GDPR does not specify by what means such information must be provided to the employees.

   Therefore, such information could be delivered to the employees by any means as long as the requirements of the Article 12 of the GDPR are met. The employer is free to choose the format or modality by which the employees would be properly informed.

   For instance:
   - data protection clause within the employment agreement;
   - appendix to the employment agreement;
   - employees' data privacy policy ...

   From a practical point of view, we recommend to provide a document, such as a privacy policy, that is separate from the employment agreement. Such privacy could be sent by email to the employees and/or freely-accessible online (on the intranet for example).

2. The Working Party 29 ("European Data Protection Board" or "EDPB") regarding "transparency" provides some guidelines with regard to this information obligation. Moreover, the French supervisory Authority (the "CNIL") also provides some recommendation regarding the way to share information to the employees.

   These are only recommendations and no particular procedure that is mandatory to comply with.

4. Is 'consent of the employee' used as a legal justification ground to process his/her data in your country, required/advised/discouraged? Can you illustrate with some examples?

In an employment context, consent of the employees is not usually used as legal basis for employees' personal data processing. In most cases, the legal basis required for processing activities is (i) the performance of the employment agreement, (ii) a legal obligation or (iii) the employer's legitimate interest.

Therefore, the employee's consent is not required for the processing of personal data regarding, in particular, payroll management, social declarations, CCTV and monitoring employee activities, as long as such personal data is processed in the context of one of the legal basis mentioned above.

On the other hand, some data processing operations require consent of the employee i.e. the use of an employee's photograph for advertising or promotional purposes.

5. The GDPR provides that a DPO benefits from dismissal protection. However, the GDPR does not provide for any penalties for the employer in case of any violation of this dismissal protection.

Can an employer in your country be sanctioned for dismissing a DPO for reasons related to his/her tasks as DPO? If yes, on what basis and what will be the penalty/ies?

The GDPR and the FDPA do not provide for any penalties for the employer in case of any violation of this DPO's dismissal protection.

However, a dismissal for reasons related to the tasks of an employee (such as the DPO) can lead to sanctions to the employers pursuant to the French Labour Law. Indeed, pursuant to Article L1232-1 of the French Labour Code, any dismissal for personal reasons must be justified by a real and serious cause.

Therefore, the DPO could claim indemnities based on a dismissal without a real and serious reason. The judge would grant the DPO indemnities, the amount of which would depend on the DPO's seniority in the company. Such indemnities range from between 1 and 20 months of salary (depending of the seniority).

6. What legal action(s) can an employee take against an employer in your country if he/she believes that his/her data protection rights are not being respected?

In France, an employee can take several legal actions against an employer in case of a violation of his/her rights.

According to the GDPR, in the event of a violation of his/her rights the employee has administrative and judicial remedies such as:

- lodge a complaint with the French supervisory Authority (the "CNIL") (GDPR, art. 77);
- a judicial remedy against the employer (acting as a data controller) before the French courts (GDPR, art. 79);
- claim for material or non-material damages with the French courts (GDPR, art. 82);
- mandate a not-for-profit body, organisation or association which is active in the field of the protection of the rights and freedoms of individuals to lodge a complaint or obtain compensation on his behalf (GDPR, art. 80).

We note that class action for data protection infringements are also possible under the FDPA (art.43 ter).

7. Does your national legislation fix a storage period for HR-related documents?

Yes

Personal data cannot be stored indefinitely by the HR services. Indeed, the GDPR indicates that personal data may only be kept for "no longer than is necessary". Therefore, the storage period must be determined according to the purpose for which the data has been collected. Once this objective has been achieved, these data should be archived, deleted or made anonymous.

The CNIL provides recommendations regarding the data storage period of the employees' personal data collected by the employer (as well as the French Labour Code and the French Civil Code).

For instance:

- in the case of a video surveillance, the storage of images may not exceed 1 month;
- data relating to payroll management can be kept for 5 years;
- data relating to premises' access must be deleted 3 months after registration;
- "social" document concerning, in particular, employment agreements, salaries, bonuses, pension information, personnel register, work accident declaration can be kept 5 years.

8. The GDPR obliges each country's supervisory data protection authority to draw up a list of the kinds of processing operations that, in its view, require a Data Protection Impact Assessment ('DPIA'), i.e. the controller's assessment of the impact of the envisaged processing operations on the protection of personal data where a type of processing is likely to result in a high risk. The supervisory data protection authority may also (but is not obliged to) draw up a list of the kinds of processing operations for which no DPIA is required.

1. Has your country's supervisory data protection authority only established a list of processing operations that require a DPIA or also a list of processing operations that do not require a DPIA?

2. Do any of these lists include HR-related processing operations?

1. On October 11, 2018 the CNIL adopted a list of processing operations that require a Data Protection Impact Assessment ("DPIA").

   We note that a list with processing operations that do not require a DPIA has not been adopted (yet).

   The list includes processing operations such as: health-related personal data, genetic data of vulnerable data subjects, large-scale processing of location data etc.

2. According to the CNIL deliberation No 2018-327 of 11 October 2018 regarding the list of types of processing operations for which a data protection impact assessment is required, DPIA is required for some HR-related processing operations.

   For instance, regarding:
   - profiling natural persons for human resources management purposes;

   - processing operations for the purpose of constantly monitoring the activity of the employees;

   - processing operations for the purpose of managing alerts regarding professional matters (whistleblowing procedure).

9. Has your country's supervisory data protection authority given any employment law-related advice or made any recommendations since the GDPR has entered into force?

Yes

The CNIL constantly updates its website and published recommendations, observations deliberations as well as guidelines related to employment matters.

Since the GDPR entered into force, the CNIL has updated or published its practice-oriented recommendations on employment privacy law implementation.

For instance, regarding:
- access to premises and control of working hours at the workplace (new recommendations);

- the biometrics at the workplace (CNIL launches a public consultation on the future regulation);

- the "Work and personal data" booklet (update – 2018 version);

- DPIA's;

- appointment of a DPO.

10. 1. Are there in your country any additional conditions, on top of what is provided for within the GDPR, to process any special categories of personal data? If so, which conditions and for which type(s) of data do they apply?

2. Does your national legislation authorize the processing of personal data relating to criminal convictions and offences? If so, when is this authorized and what are the appropriate safeguards that should be complied with (if any)?

Yes

1. In France, the FDPA provides additional conditions, on top of what is provided within the GDPR, for the processing of health data and biometric data.

   - Article 8 of the FDPA indicates that processing biometric data for the purpose of uniquely identifying a natural person is prohibited. However, the FDPA determine additional conditions (on top of the GDPR) for processing such data (see question 1 above).

   - Chapter IX of the FDPA provides specific rules for the processing of health data (e.g. the processing of health data justified by a purpose in the public interest is still subject to a CNIL's authorisation).

2. In France, the FDPA provides additional conditions, on top of what is provided within the GDPR, for the processing of data related to criminal convictions and offences and also for the processing carried out for the prevention and detection of criminal offences.

   - Article 9 of the FDPA indicates that processing of data related to criminal convictions and offences can now be carried out by an extended list of persons such as (1) courts, public authorities and legal persons operating a public service, (2) judicial officer, or (3) victims in criminal proceedings. We note that such list does not include employers.

   - Chapter XIII of the FDPA provides specific rules for the processing operations carried out for the purposes of prevention, detection or enforcement of criminal offences (e.g. such processing is still subject to a CNIL's authorisation and can be only carried out by public authorities).

GERMANY

/ Prof. Dr. Martin Reufels
Partner
+49 221 20 52 331
m.reufels@heuking.de

/ Regina Glaser
Partner
+49 211 600 55 276
r.glaser@heuking.de

1. As an EU Regulation, the GDPR is directly applicable and must not be implemented into national legislation. However, the GDPR includes certain articles that give Member States the opportunity to have specific national legislation in execution of the GDPR. This is, for instance, the case for the processing of employee personal data.

1. Has your country made use of this opportunity to have specific national rules regarding the processing of employee personal data? If so, please comment on these rules.

2. If not, has your country adopted other national data protection legislation in execution of the GDPR that could be relevant in an HR context? If so, please give a short bullet-point overview of the relevant provisions.

Germany has made use of this opportunity in section 26 of the Federal Data Protection Act.

The consent of an employee has to be in writing and has to be freely given. Benefits for the employee and joint interests have to be taken into account when assessing the freedom of will.

The section allows the processing of data on the basis of collective agreements.

2. Does any other employment-related privacy legislation exist in your country (not necessarily in execution of the GDPR)? Has the GDPR impacted this existing privacy legislation?

Because of the GDPR, the old Federal Data Protection Act was replaced by a new one. It came into force at the same time as the GDPR. The terminology was adjusted to the one used by the GDPR. The legislator added the possibility of processing of personal data to exercise or satisfy rights and obligations of employees' representation. Other changes were not made.

3. The information obligation of employers (data controllers) towards their employees has been extended under the GDPR. Therefore, the current information clauses/policies will probably no longer be sufficient.

1. By what means (e.g. (an annex to) the employment contract, work rules, a policy) would you recommend employers in your country provide employees with this extended information?

2. Should any particular procedure be complied with?

I would recommend an annex to the employment contract or a simple handout about the kind of personal data processed. I would also recommend that the employees sign a receipt when receiving the information.

4. Is 'consent of the employee' used as a legal justification ground to process his/her data in your country, required/advised/discouraged? Can you illustrate with some examples?

Personal data of employees can be processed on the basis of consent, but it is not needed for all processing in the employment relationship. You don't need the express consent for processing all data needed to carry out the employment contract as it is already allowed by the law. For example, the employer is allowed to process some personal data to exercise rights or comply with legal obligations derived from labour law, social security and social protection law.

On the other hand, there are situations where the employer has to ask for the employee's consent. In those cases, the consent has to be given freely. It is presumed to be given freely in particular if it is associated with a legal or economic advantage for the employee, or if the employer and employee are pursuing the same interests. For example, a candidate to a job can agree that his data is saved in order to be taken into consideration in case of another vacancy. He could also consent to his data to be saved in a group-wide database so he can participate in talent promotion programmes.

A better way though would be to regulate those issues through a collective agreement as the employee can take back his consent at any time. Also it can be quite difficult to proof the employee consented freely.

5. The GDPR provides that a DPO benefits from dismissal protection. However, the GDPR does not provide for any penalties for the employer in case of any violation of this dismissal protection.

Can an employer in your country be sanctioned for dismissing a DPO for reasons related to his/her tasks as DPO? If yes, on what basis and what will be the penalty/ies?

The DPO can only be dismissed from his functions as DPO for causes which allow instant dismissal for cause (sec. 626 of the German Civil Code).

In Germany, if the designation of a data protection officer is compulsory, he can only be terminated instantly for cause. In this case the DPO can sue his employer in order to continue working there. But literature asks critically whether this is compatible with the GDPR.

The German Federal Data Protection Act refers for the possibility to penalize the employer to section 83 paragraph 4 of the GDPR which penalizes any infringement of the DPO's dismissal protection with an administrative fine.

6. What legal action(s) can an employee take against an employer in your country if he/she believes that his/her data protection rights are not being respected?

The employee can sue the employer in application of section 79 paragraph 1 and section 82 paragraph 1 GDPR.

Furthermore, the employee can sue the employer if the latter violates the employee's personal rights in application of section 823 of the German Civil Code.

7. Does your national legislation fix a storage period for HR-related documents?

German legislation fixes several storage periods for HR-related documents. Those periods can be found in very different acts. They differ depending on the purpose they are stored for. They can for example be found in the Social Security Code and in the Income Tax Act.

8. The GDPR obliges each country's supervisory data protection authority to draw up a list of the kinds of processing operations that, in its view, require a Data Protection Impact Assessment ('DPIA'), i.e. the controller's assessment of the impact of the envisaged processing operations on the protection of personal data where a type of processing is likely to result in a high risk. The supervisory data protection authority may also (but is not obliged to) draw up a list of the kinds of processing operations for which no DPIA is required.

1. Has your country's supervisory data protection authority only established a list of processing operations that require a DPIA or also a list of processing operations that do not require a DPIA?

2. Do any of these lists include HR-related processing operations?

In Germany each federal state has its own supervisory data protection authority. In addition to that, the Federal Republic of Germany has one too. Each of them published a list of processing operations for which a DPIA is needed. A coordinated list was published later on by the joint Data Protection Committee. The authorities point out that those lists are not conclusive.

They did not though publish any so called white lists.

This coordinated list includes two HR-related processing operations: a DPIA is required to implement data-loss-prevention systems which generates employees' profiles. This can for example be used to find out about unwanted employees' behaviour. A DPIA is also required to geo-localize employees.

9. Has your country's supervisory data protection authority given any employment law-related advice or made any recommendations since the GDPR has entered into force?

The Data Protection Committee published advice concerning Employee Data Protection. This can be found on the websites of all 17 data protection authorities.

10. 1. Are there in your country any additional conditions, on top of what is provided for within the GDPR, to process any special categories of personal data? If so, which conditions and for which type(s) of data do they apply?

2. Does your national legislation authorize the processing of personal data relating to criminal convictions and offences? If so, when is this authorized and what are the appropriate safeguards that should be complied with (if any)?

To my knowledge there are no further conditions for any special categories of personal data.

Section 4 paragraph 3 allows the processing of data obtained through video surveillance of publicly accessible spaces if necessary to prevent threats to state and public security and to prosecute crimes.

In accordance with section 26 paragraph 1 FDPA employees' personal data may be processed to detect crimes only if there is a documented reason to believe the data subject has committed a crime while employed, the processing of such data is necessary to investigate the crime and is not outweighed by the data subject's legitimate interest in not processing the data, and in particular the type and extent are not disproportionate to the reason.

Furthermore, section 40 paragraph 3 allows the processing of data to the supervisory authority and the transfer to other supervisory authorities if processing is necessary to prosecute crimes or administrative offences, to carry out or enforce punishment or measures as referred to in Section 11 of the Criminal Code or educational or disciplinary measures as referred to in the Juvenile Court Act or to enforce fines.

POLAND

/ Marcin Wujczyk Ph. d.
attorney at law
+48 12 290 86 20
marcin.wujczyk@wardynski.com.pl

1. As an EU Regulation, the GDPR is directly applicable and must not be implemented into national legislation. However, the GDPR includes certain articles that give Member States the opportunity to have specific national legislation in execution of the GDPR. This is, for instance, the case for the processing of employee personal data.

1. Has your country made use of this opportunity to have specific national rules regarding the processing of employee personal data? If so, please comment on these rules.

2. If not, has your country adopted other national data protection legislation in execution of the GDPR that could be relevant in an HR context? If so, please give a short bullet-point overview of the relevant provisions.

1. **Yes.**

The Labour Code has provisions that permit an employer to require an applicant to provide the following personal data:

- name(s) and surname;
- names of parents;
- date of birth;
- place of residence (mailing address);
- education;
- employment record.

An employer can require an employee to provide the following data in addition to the personal data specified above:

- other personal data of an employee, and names and surnames and dates of birth of children, if necessary to exercise special rights to which an employee is entitled pursuant to labour law,

- the PESEL identification number assigned to an employee by the Government Information Centre of the Common Electronic System of Population Register (RCI PESEL).

Additionally, it is planned to add regulations with respect to processing employee personal data. Pursuant to them, it will be possible to process all personal data provided by an employee at the consent of the employee.

2. The Act of May 10, 2018 on the protection of personal data is meant to implement GDPR. It contains mainly provisions concerning the inspections supervisory data protection authority to check compliance of employers with personal data protection regulations.

2. Does any other employment-related privacy legislation exist in your country (not necessarily in execution of the GDPR)? Has the GDPR impacted this existing privacy legislation?

There are works in progress to amend existing legislation to implement GDPR.

The Labour Code has provisions on monitoring employees. Pursuant to the amended regulations, if that is necessary to ensure the safety of employees or protection of property, or production control, or confidentiality of information the disclosure of which could harm employer interests, an employer

can have special supervision of premises of the establishment or the area around the establishment in the form of technical measures that enable video recording (monitoring).

Recently, there have been amendments to the Act of April 12, 2018 on the principles of checking police records of persons applying for employment and those employed in the financial sector. The possibility to demand a certificate of lack of convictions applies to employees in the financial sector who are employed in positions involving:

- managing the property of businesses, or of third parties;
- accessing information protected by the law,
- making decisions that risk loss of property of such business or of third parties and of causing other significant harm to the business or to third parties.

The record of convictions can only refer to the offences specified in the Act.

3. The information obligation of employers (data controllers) towards their employees has been extended under the GDPR. Therefore, the current information clauses/policies will probably no longer be sufficient.

1. By what means (e.g. (an annex to) the employment contract, work rules, a policy) would you recommend employers in your country provide employees with this extended information?

2. Should any particular procedure be complied with?

1. The recommended solution, which also is common in Poland, is delivering information about personal data processing in the form of a separate document. An employee should confirm reading it. An alternative form is implementing a personal data protection policy that contains the required information about personal data processing. It is not recommended to conclude a separate annex to an employment contract because any change of data will mean it is necessary to sign another, amending annex.

2. The regulations do not have a special procedure to fulfil information obligations. However, it is advised that an employee confirm in writing of having become aware of the information that is provided. Such declaration would then be put on the personnel file.

4. Is 'consent of the employee' used as a legal justification ground to process his/her data in your country, required/advised/discouraged? Can you illustrate with some examples?

The fact that an employer can obtain personal data after consent of an employee causes disputes in Polish jurisprudence and litigation. Some opine that written consent of an employee is a breach of the employee's rights and the freedom to make a decision (judgment of the Supreme Administrative Court of the 1.12.2009, I OSK 249/09) because of the lack of freedom of an employee to make decisions about an employment relationship; they concluded that the consent is not free consent. The court stated in that judgment that ...such view is supported by the dependence of the employee on the employer. Lack of equality in the employer-employee relations raises doubt concerning the voluntary aspect of expressing consent to collecting and processing personal (biometric) data. Because of that, the legislative authority limited in the provisions of the Labour Code the list of data that the employer can demand from the employee. Considering that the fact that the employee expressed consent is a circumstance that justifies collecting data other than that listed in the Labour Code would be a circumvention of these provisions.... This interpretation is subject to change. It is planned to amend the Labour Code to permit personal data processing after an employee consents.

5. The GDPR provides that a DPO benefits from dismissal protection. However, the GDPR does not provide for any penalties for the employer in case of any violation of this dismissal protection.

Can an employer in your country be sanctioned for dismissing a DPO for reasons related to his/her tasks as DPO? If yes, on what basis and what will be the penalty/ies?

Terminating a contract of employment for that cause could be considered to be unjustified termination; an employee would be entitled to require reinstatement or compensation (up to 3 months' pay). However, there the regulations do not have penal or administrative sanctions that could be imposed on an employer for dismissing a DPO for reasons related to the tasks as DPO.

6. What legal action(s) can an employee take against an employer in your country if he/she believes that his/her data protection rights are not being respected?

An employee can sue an employer under section 79 (1) and section 82 (1) of GDPR.

Furthermore, an employee can sue an employer if the latter infringes the employee's personal rights in application of section 23 and 24 of the Polish Civil Code and demand:

- the employer cease infringing the rights.
- rectification of harm (if it was incurred).
- compensation (if the infringement caused harm, or
- an apology.

The employee will have the right to terminate employment because of infringement related to personal data processing.

7. Does your national legislation fix a storage period for HR-related documents?

Yes.

The periods of storage depend on the type of employee documents; for example:

- Contracts (engagements, severance, etc.), time records (work hours, rest periods, vacation/ sick/holiday, etc.), data and personnel files; the period depends on an employee's date of hire:
  - After Jan. 1, 2019: minimum 10 years
  - Between Jan. 1999 - Dec. 2018: Minimum 50 years, or a shortened minimum of 10 years if employer submits information report to Social Security Institution
  - Before 1999: minimum 50 years
- Injury and illness incident reports – the minimum period is 10 years
- Tax records – 5 years

8. The GDPR obliges each country's supervisory data protection authority to draw up a list of the kinds of processing operations that, in its view, require a Data Protection Impact Assessment ('DPIA'), i.e. the controller's assessment of the impact of the envisaged processing operations on the protection of personal data where a type of processing is likely to result in a high risk. The supervisory data protection authority may also (but is not obliged to) draw up a list of the kinds of processing operations for which no DPIA is required.

1. Has your country's supervisory data protection authority only established a list of processing operations that require a DPIA or also a list of processing operations that do not require a DPIA?
2. Do any of these lists include HR-related processing operations?

1. Polish supervisory data protection authority only established a list of processing operations that require a DPIA
2. The list of processing operations that require a DPIA includes the following HR-related processing operations:
   - systems for the monitoring of employee worktime and of the tools used by employees (e-mail, the Internet),
   - processing biometric data of employees to identify or verify identities in accessing control systems, e.g., for the purpose of entering specific areas, rooms or obtaining access to certain accounts in the IT system, for example, to order a transaction in the IT system or to withdraw cash from an ATM, etc.

9. Has your country's supervisory data protection authority given any employment law-related advice or made any recommendations since the GDPR has entered into force?

Yes.

Polish supervisory data protection authority has published the guide "Personal data protection at the workplace. Guide for employers". The position stating that the resumes of applicants collected in recruitment are to be destroyed immediately after the end of recruitment was controversial. It differs from the opinion of most Polish lawyers who believe that CVs can be stored for the period of limitation on the claims that an applicant could make because of not being employed; e.g., discrimination claims.

10. 1. Are there in your country any additional conditions, on top of what is provided for within the GDPR, to process any special categories of personal data? If so, which conditions and for which type(s) of data do they apply?

2. Does your national legislation authorize the processing of personal data relating to criminal convictions and offences? If so, when is this authorized and what are the appropriate safeguards that should be complied with (if any)?

1. Data relating to convictions and offences can be processed only if permitted by the Act. See comments below.

2. Processing data relating to convictions and offences requires express authorisation under the Act; the data cannot be processed, e.g., after consent of an employee. Currently, such data can be processed, among others, with respect to police officers, detectives, teachers, security workers, tax inspection employees, tourist guides, and employees of self-government authorities and financial institutions.

The legislation has safeguards for processing such information:

- Data is obtained only from the information from the National Criminal Records.
- Only information about certain types of offences that are relevant to the work performed can be processed.
- Only a limited group of persons can have access to the data.

Data should be removed after the offence is erased from the register..

SPAIN

1. As an EU Regulation, the GDPR is directly applicable and must not be implemented into national legislation. However, the GDPR includes certain articles that give Member States the opportunity to have specific national legislation in execution of the GDPR. This is, for instance, the case for the processing of employee personal data.

1. Has your country made use of this opportunity to have specific national rules regarding the processing of employee personal data? If so, please comment on these rules.

2. If not, has your country adopted other national data protection legislation in execution of the GDPR that could be relevant in an HR context? If so, please give a short bullet-point overview of the relevant provisions.

1. Spanish Data Protection Bill, to be processed by the Senate, includes a provision regarding the creation and maintenance of whistleblowing systems.

   Additionally, it sets out several provisions in relation to the following rights regarding employees:

   - The right of the employees to the protection of their privacy in the use of digital devices made available to them by their employer.
   - The right of employees to digital disconnection.
   - The right of the employees to the protection of their privacy in relation to the use of video surveillance and sound recording devices in the workplace.
   - The right of employees to privacy regarding the use of geolocation systems in the context of the employment relationship.
   - The right of employees to establish additional digital rights in collective agreements.

2. There are other regulations that set out obligations regarding the processing of personal data, such as the Law on the Prevention of Money Laundering and the Financing of Terrorism, the Law on the Protection of Minors, among others. Said regulations detail several cases in which the employer must process information in relation to criminal convictions regarding the employee.

/ Ángel Olmedo Jiménez
Partner
+34 91 514 52 00
angel.olmedo.jimenez@garrigues.com

2. Does any other employment-related privacy legislation exist in your country (not necessarily in execution of the GDPR)? Has the GDPR impacted this existing privacy legislation?

Law 31/1991 on Labour Risk Prevention imposes on the company the performance of a set of activities with the aim of avoiding or reducing risks arising from the job, for which it is necessary to process personal data relating to employees. This regulation sets out the need to process special categories of personal data such as health information. It also provides several events in which personal data may be transferred to third parties such as health authorities, labour authority, or judges and courts.

Royal Decree 2/2015 that approves the Law on the Statute of Workers empowers companies to carry out checks in the event of illness or accident at work resulting in absence from work. This control shall be carried out by means of a medical examination which entails the processing of personal data.

3. The information obligation of employers (data controllers) towards their employees has been extended under the GDPR. Therefore, the current information clauses/policies will probably no longer be sufficient.

1. By what means (e.g. (an annex to) the employment contract, work rules, a policy) would you recommend employers in your country provide employees with this extended information?

2. Should any particular procedure be complied with?

1. It would be advisable to include this information through an annex to the employment contract.

2. Any means will be valid as long as the complete information is given to the employees and the controller can prove that each and all employees have been duly informed.

   For new employees, we recommend providing a first layer of information in the body of the employment contract and a second layer as an annex to said contract.

   For employees that signed their contract before May 25, 2018, we recommend choosing one of the two following options:

   - To provide the employees with the complete information in paper form and to ask the employees to sign receipt of the document.

   - To send the first layer of information via e-mail to all the employees and provide them in said e-mail with a link to the second layer including the complete information.

   Among these two options we would recommend implementing the second procedure provided that it is easier to prove the fulfilment of the duty to inform (please note that if it is provided in paper form there may be employees that do not sign reception of the document).

4. Is 'consent of the employee' used as a legal justification ground to process his/her data in your country, required/advised/discouraged? Can you illustrate with some examples?

The use of consent of the employee as a ground to process his or her personal data is discouraged in Spain. As mentioned in previous questions, the performance of a contract shall not be subject to the consent of the data subject to the processing of personal data.

The Spanish Data Protection Authority has not issued guidelines on this issue. However, it has provided by means of its answers to the Frequently Asked Questions that consent shall be used in limited cases in the context of employment relationships. Therefore, it may only be used in determined events such as: to receive newsletters, to be part of advertising activities, to be part of social benefits programs, to use the employee's fingerprint to enable access, etc. Consequently, it shall not be used as the legal ground to legitimize the processing of personal data that is necessary for the performance of the contract.

5. The GDPR provides that a DPO benefits from dismissal protection. However, the GDPR does not provide for any penalties for the employer in case of any violation of this dismissal protection.

Can an employer in your country be sanctioned for dismissing a DPO for reasons related to his/her tasks as DPO? If yes, on what basis and what will be the penalty/ies?

There are no local sanctions apart from those established in the GDPR.

Although there is no local regulation in this respect, there could be a risk that a DPO's dismissal could be declared as null and void by a labour court as he/she could be treated as a workers' representative (i.e. in terms of their special protected status against dismissals).

6. What legal action(s) can an employee take against an employer in your country if he/she believes that his/her data protection rights are not being respected?

In case his or her rights are not being respected, the employee may lodge a complaint with the Spanish Data Protection Authority. The Spanish Data Protection Authority shall then decide whether the complaint is accepted for processing.

In case the complaint is not accepted for processing or if the decision is not favourable for the employee, the employee may lodge an appeal with the contentious-administrative jurisdiction.

7. Does your national legislation fix a storage period for HR-related documents?

The Spanish data protection legislation does not provide a storage period for HR-related documents. Said period shall be subject to the national employment, tax and commercial legislation, as well as any other that may affect HR-related documents.

8. The GDPR obliges each country's supervisory data protection authority to draw up a list of the kinds of processing operations that, in its view, require a Data Protection Impact Assessment ('DPIA'), i.e. the controller's assessment of the impact of the envisaged processing operations on the protection of personal data where a type of processing is likely to result in a high risk. The supervisory data protection authority may also (but is not obliged to) draw up a list of the kinds of processing operations for which no DPIA is required.

1. Has your country's supervisory data protection authority only established a list of processing operations that require a DPIA or also a list of processing operations that do not require a DPIA?

2. Do any of these lists include HR-related processing operations?

1. The Spanish Data Protection Authority has not established yet either a list of the processing operations that require a DPIA or a list of the processing operations that do not require a DPIA.

2. N/A.

9. Has your country's supervisory data protection authority given any employment law-related advice or made any recommendations since the GDPR has entered into force?

The Article 29 Working Party has issued several guidelines according to which, when a data subject is in a situation of dependence on the data controller, due to the nature of the relationship, there may be a strong presumption that freedom to consent is limited in such contexts.

Accordingly, the Spanish Data Protection Authority has determined that consent shall be limited in the context of employment relationships.

10.

1. Are there in your country any additional conditions, on top of what is provided for within the GDPR, to process any special categories of personal data? If so, which conditions and for which type(s) of data do they apply?

2. Does your national legislation authorize the processing of personal data relating to criminal convictions and offences? If so, when is this authorized and what are the appropriate safeguards that should be complied with (if any)?

The Spanish Data Protection Bill provides that, in order to avoid discrimination, the mere consent of the data subject shall not be enough to lift the prohibition on the processing of data for the main purpose of identifying the data subject's beliefs, trade-union membership, religion, sexual orientation or racial or ethnic origin.

This information may be processed under the grounds of any other legal bases.

The candidate's criminal background may only be checked where required by law. There are certain restricted business sectors in which the law requires the absence of criminal record on the part of the employee. Therefore, criminal background must only be checked within the following sectors: (i) public administrations, (ii) police and the army, (iii) top executives of financial institutions, (iv) brokers, (v) education and other sectors related to minors, (vi) anti money laundering, and (vii) private security.

SWEDEN

/ Peter Nordbeck
Partner
+46 709 25 25 01
peter.nordbeck@delphi.se

/ Felix Makarowski
Associate
+46 709 25 25 27
felix.makarowski@delphi.se

1. As an EU Regulation, the GDPR is directly applicable and must not be implemented into national legislation. However, the GDPR includes certain articles that give Member States the opportunity to have specific national legislation in execution of the GDPR. This is, for instance, the case for the processing of employee personal data.

1. Has your country made use of this opportunity to have specific national rules regarding the processing of employee personal data? If so, please comment on these rules.

2. If not, has your country adopted other national data protection legislation in execution of the GDPR that could be relevant in an HR context? If so, please give a short bullet-point overview of the relevant provisions.

1. No.

2. The Swedish Data Protection Act (SFS 2018:218) was adopted in execution of the GDPR. Of particular interest from an HR perspective is the following (Chapter 3 Section 2):

   - Special categories of personal data may be processed in accordance with Article 9.2 b of the GDPR.

   - Such special categories of personal data include data concerning health and union membership of an employee, which may be processed to enable administration of the employee's pay, sick leave, insurance and pension etc.

   - Disclosure to a third party of personal data which is processed on the basis of Chapter 3 Section 2 of the Data Protection Act is only allowed if the employer has an obligation to disclose the data under employment law or within the field of social security or if the employee expressly has consented to the disclosure.

2. Does any other employment-related privacy legislation exist in your country (not necessarily in execution of the GDPR)? Has the GDPR impacted this existing privacy legislation?

There is yet no specific employment-related privacy legislation in Sweden, even though legislative initiatives have been taken.

A new Act on camera surveillance has been enacted, referring to the provisions of the GDPR as regards processing of personal data.

3. The information obligation of employers (data controllers) towards their employees has been extended under the GDPR. Therefore, the current information clauses/policies will probably no longer be sufficient.

1. By what means (e.g. (an annex to) the employment contract, work rules, a policy) would you recommend employers in your country provide employees with this extended information?

2. Should any particular procedure be complied with?

Same as for Belgium.

4. Is 'consent of the employee' used as a legal justification ground to process his/her data in your country, required/advised/discouraged? Can you illustrate with some examples?

No, consent is rarely used and not advised. This as a consent shall be given freely and due to the possibility for the employee to at any time recall the consent. Given the imbalance of authority within an employer an employee relationship, consent is therefore seldom given freely.

It should be mentioned, however, that under Swedish law applicable prior to the GDPR, the Swedish Data Protection Authority recommended consent as a legal justification ground for certain processing within the employment context, such as for evaluation of employees' performance. Following the entering into force of the GDPR, the Swedish Data Protection Authority most likely is no longer in support of this view.

5. The GDPR provides that a DPO benefits from dismissal protection. However, the GDPR does not provide for any penalties for the employer in case of any violation of this dismissal protection.

Can an employer in your country be sanctioned for dismissing a DPO for reasons related to his/her tasks as DPO? If yes, on what basis and what will be the penalty/ies?

As described above regarding Belgium, Swedish legislation does not provide for any additional sanctions for the employer in the case of a DPO's dismissal for reasons related to his/her tasks as DPO. Hence, until further provisions or case law clarifications are issued, a DPO may claim damages based on Swedish employment legislation in cases of wrongful termination of employment in the same way as other employees.

6. What legal action(s) can an employee take against an employer in your country if he/she believes that his/her data protection rights are not being respected?

If an employee considers that his/her rights according to the GDPR are violated, the individual may:

- Report the breach to the Swedish Data Protection Authority.
- Claim damages by a court proceeding.

7. Does your national legislation fix a storage period for HR-related documents?

The following rules of thumb may be applied:

Job-seekers:

- The personal data of a job seeker should immediately be deleted when the application process has ended, unless the applicant has been informed that his/her personal data will be processed further.
- If the applicant has consented to processing of personal data, the data may typically be kept until the consent is withdrawn.
- Regardless of whether the applicant has consented to the processing of personal data, an employer may keep personal data for up to 2 years on the basis of defence of a discrimination law suit under the Swedish Discrimination Act in relation to the application process.

Employees:

- Name, personal identity number and term of employment may be kept indefinitely under the Swedish Employment Protection Act.
- Salaries and payments of salaries may be stored for 7 years for accounting purposes.
- Personal data about pensions may be kept for 10 years.
- Information about the term of employment (start and end date) may be kept indefinitely. Other personal data related to termination of employment may be kept for 7 years for accounting purposes.
- Personal data such as grades, references, etc. may be kept for up to 2 years under the rules of the Swedish Discrimination Act.
- Information about vacations may be kept for 10 years if its relevant to the pension of the employee or for 7 years for accounting purposes.
- Information about sickness benefits may be kept for 10 years if its relevant to the pension of the employee or for 7 years for accounting purposes.
- Other personal data should be deleted when the employment ends.

8. The GDPR obliges each country's supervisory data protection authority to draw up a list of the kinds of processing operations that, in its view, require a Data Protection Impact Assessment ('DPIA'), i.e. the controller's assessment of the impact of the envisaged processing operations on the protection of personal data where a type of processing is likely to result in a high risk. The supervisory data protection authority may also (but is not obliged to) draw up a list of the kinds of processing operations for which no DPIA is required.

1. Has your country's supervisory data protection authority only established a list of processing operations that require a DPIA or also a list of processing operations that do not require a DPIA?

2. Do any of these lists include HR-related processing operations?

The Swedish Data Protection Authority will provide a list of examples of processing activities which require a DPIA, but underlines that the list will not be exhaustive.

The guidelines give a few examples of when a DPIA is not needed, such as news letters or a web page for e-commerce.

9. Has your country's supervisory data protection authority given any employment law-related advice or made any recommendations since the GDPR has entered into force?

The Swedish Data Protection Authority has issued a booklet on data protection for small companies. The Swedish Data Inspection Authority has also published information for employers on its website. As a result of the entering into force of the GDPR, the Swedish Data Protection Authority has provided advice on the posting of employees' photos on the employer's web site.

10.

1. Are there in your country any additional conditions, on top of what is provided for within the GDPR, to process any special categories of personal data? If so, which conditions and for which type(s) of data do they apply?

2. Does your national legislation authorize the processing of personal data relating to criminal convictions and offences? If so, when is this authorized and what are the appropriate safeguards that should be complied with (if any)?

1. Within the employment context, it should be mentioned (although personal identification number is not included in the definition of special categories of personal data) that the specific conditions regarding processing of personal identification number that applied under the previous legislation have been implemented in the Swedish Data Protection Act supplementing the GDPR.

2. As a general rule, Swedish law does not permit processing of personal data relating to criminal convictions and offences. In principle, employers will not be able to retain or process the criminal record of an employee or an applicant. The employer may however ask to view the information without processing it. Some exemptions from the prohibition do however apply, for example if it is necessary for the establishment, exercise or defence of legal claims or if it is necessary to fulfil a legal obligation set out in law.

THE NETHERLANDS

/ Cara Pronk
Senior associate
+31 20 6789 503
pronk@vandoorne.com

/ Els de Wind
Partner
+31651506662
wind@vandoorne.com

1. As an EU Regulation, the GDPR is directly applicable and must not be implemented into national legislation. However, the GDPR includes certain articles that give Member States the opportunity to have specific national legislation in execution of the GDPR. This is, for instance, the case for the processing of employee personal data.

1. Has your country made use of this opportunity to have specific national rules regarding the processing of employee personal data? If so, please comment on these rules.

2. If not, has your country adopted other national data protection legislation in execution of the GDPR that could be relevant in an HR context? If so, please give a short bullet-point overview of the relevant provisions.

1. The Netherlands did not (yet) use article 88 of the GDPR to have additional national legislation on the processing of employee personal data.

2. In the Netherlands the Dutch GDPR Implementation Act *(Uitvoeringswet AVG)* came into force on 25 May 2018. The act provides additional rules on, amongst others, the processing of special categories of personal data. This can be relevant in an HR context since certain personal employee data, such as information regarding health of employees, membership of a trade union and the citizen service number *(burgerservicenummer),* qualify as special categories of personal data. Articles 22 to 30 and 46 of the Dutch GDPR Implementation Act provide additional conditions under which the processing of special categories of personal data is allowed.

2. Does any other employment-related privacy legislation exist in your country (not necessarily in execution of the GDPR)? Has the GDPR impacted this existing privacy legislation?

No, the GDPR replaced the Dutch Data Protection Act *(Wet bescherming persoonsgegevens).*

3. The information obligation of employers (data controllers) towards their employees has been extended under the GDPR. Therefore, the current information clauses/policies will probably no longer be sufficient.

1. By what means (e.g. (an annex to) the employment contract, work rules, a policy) would you recommend employers in your country provide employees with this extended information?

2. Should any particular procedure be complied with?

1. Even before execution of the GDPR we recommended employers to provide an HR privacy statement to their employees in order to be compliant with the information obligations under then existing Dutch privacy legislation.

   Due to the extended information obligations under the GDPR (such as the right to be forgotten and the right to data portability) and the high fines for data protection violations (up to EUR 20 million). We recommend employers to adjust their current HR privacy statements to the extended information obligations. Employers should keep in mind that for the introduction or amendment of the HR privacy statement prior consent of the works council might be required.

   The extended information obligations also apply to job applicants. Therefore, we would recommend (future) employers to provide a (separate) privacy statement to job applicants as well. This can be a separate statement or can be done by implementing in the application form a hyperlink to the privacy statement at the homepage of the employer. Employers should keep in mind that for the introduction or amendment of the (job applicants) privacy statement prior consent of the works council might be required.

2. The GDPR and the Dutch GDPR Implementation Act do not include a specific prescribed procedure by which information should be provided to the employees.

4. Is 'consent of the employee' used as a legal justification ground to process his/her data in your country, required/advised/discouraged? Can you illustrate with some examples?

Under Dutch law consent of the employee is not accepted as a lawful basis for the processing of employee personal data. According to Article 7 GDPR consent should be freely given and does not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller. Therefore, consent as a legal basis for processing of employee personal data is problematic in the employment relationship.

The employee can at all times withdraw the given consent.

The Working Party 29 (now the European Data Protection Board) is of the opinion that in exceptional circumstances the employer can rely on consent of the employee as a lawful basis for the processing of employee personal data. For instance, employees can be asked to give consent for the recording of a film at the workplace, if they were offered the opportunity to work somewhere where no recording takes place. This example illustrates that: (i) if employees were given equivalent desks elsewhere in the building; and (ii) there are no adverse consequences at all whether or not the employee gives consent, consent sometimes can be considered as 'freely given'.

5. The GDPR provides that a DPO benefits from dismissal protection. However, the GDPR does not provide for any penalties for the employer in case of any violation of this dismissal protection.

Can an employer in your country be sanctioned for dismissing a DPO for reasons related to his/her tasks as DPO? If yes, on what basis and what will be the penalty/ies?

Article 38 GDPR and article 7:670 sub 10 under d Dutch Civil Code *(Burgerlijk Wetboek)* provide that a DPO enjoys dismissal protection. The DPO cannot be dismissed by the employer during his employment as DPO. Under certain conditions such as bankruptcy of the employer, when the DPO has reached the state pension age *(AOW-gerechtigde leeftijd)* or the DPO agrees on the termination of his employment, the DPO can be dismissed. Moreover, the employer can ask the Dutch court to terminate the DPO's employment and the court may do so in case the dismissal ground(s) stated are not related to the function of DPO.

Dutch legislation does not provide any sanctions or penalties for the employer in case of unlegislated dismissal of the DPO. The DPO can file a request with the Dutch court to nullify the dismissal or to award fair compensation *(billijke vergoeding)* to the employee.

6. What legal action(s) can an employee take against an employer in your country if he/she believes that his/her data protection rights are not being respected?

The employee may lodge a complaint with the Dutch Data Protection Authority *(Autoriteit Persoonsgegevens)*. The Dutch Data Protection Authority will inform the employee on the progress and the outcome of the complaint including the possibility of a judicial remedy.

If the employees has an urgent interest by having the infringement of his rights ceased, the employee could request the court to give a preliminary ruling in summary proceedings.

The employee may start legal proceedings against his employer based on breach of good employment practices (article 7:611 Dutch Civil Code) and may claim material and/or non-material damages.
The employee may mandate certain non-profit-bodies, organizations or associations to lodge a complaint with the Dutch Data Protection Authority or start legal proceedings on his/her behalf against the employer.

7. Does your national legislation fix a storage period for HR-related documents?

Yes, Dutch legislation provides some fix storage periods for HR-related documents:

- Personal data relating to tax issues can be stored for a maximum period of seven years after the termination of employment.
- The payroll tax statement and a copy of the identity document can be stored for a maximum period of five years after the termination of employment.

For other HR-related documents no statutory fix storage period is applicable. Therefore, the general rule applies that such documents can be stored for a maximum period of five years after the termination of employment. For documents relating to job-applicants applies a maximum storage period of 4 weeks after the end of the selection procedure.

8. The GDPR obliges each country's supervisory data protection authority to draw up a list of the kinds of processing operations that, in its view, require a Data Protection Impact Assessment ('DPIA'), i.e. the controller's assessment of the impact of the envisaged processing operations on the protection of personal data where a type of processing is likely to result in a high risk. The supervisory data protection authority may also (but is not obliged to) draw up a list of the kinds of processing operations for which no DPIA is required.

1. Has your country's supervisory data protection authority only established a list of processing operations that require a DPIA or also a list of processing operations that do not require a DPIA?

2. Do any of these lists include HR-related processing operations?

The Dutch Data Protection Authority has established a list for processing operations that at all times do require a DPIA. The list is not exhaustive and employers need to determine if their processing operations contain high privacy risks.

HR-related processing operations included in the list are:

- camera surveillance by the employer in order to combat theft and fraud of employees;
- processing a black list of employees (for example used in the health care sector and employment agency industry);
- on a large scale and/or systemically screening of employee activities, for instance by controlling e-mail, internet usage and following employees via GPS systems.

9. Has your country's supervisory data protection authority given any employment law-related advice or made any recommendations since the GDPR has entered into force?

It depends what is meant by "advice". On the website of the Dutch Protection Authority on many subjects explanation and advice is to be found.

10.

1. Are there in your country any additional conditions, on top of what is provided for within the GDPR, to process any special categories of personal data? If so, which conditions and for which type(s) of data do they apply?

2. Does your national legislation authorize the processing of personal data relating to criminal convictions and offences? If so, when is this authorized and what are the appropriate safeguards that should be complied with (if any)?

1. No. However, the Dutch GDPR Implementation Act (Uitvoeringswet AVG) provides exceptions to the conditions under which special categories of personal data can be processed.

2. The processing of personal data relating to criminal convictions and offences is in most cases not allowed. Usually, it is sufficient if the employee provides the employer with a Certificate of Conduct *(Verklaring Omtrent Gedrag (VOG))*. The employee can obtain a Certificate of Conduct by filing a request at the Ministry of Justice. Subsequently, The Ministry of Justice will conduct a screening of the employee and in case of a positive outcome provides the employee with the certificate.

   The employer is allowed to process personal data relating to criminal convictions and offences to the extent necessary to meet someone's request to take a certain decision regarding him or her, or to provide services to the employer. For instance if the applicant applies for a integrity position the processing of personal data relating to criminal convictions and offences by the (future) employer might be necessary.

   The employer may process personal data relating to criminal offences to protect its own interest. For example an employer may process camera surveillance data if a criminal offence such as theft was recorded.

   It should be kept in mind that for the processing of data obtained by camera surveillance consent of the works council might be required.

UK

/ Kevin McCavish
Partner
+44 (0) 118 965 8802
kevin.mccavish@shoosmiths.co.uk

1. As an EU Regulation, the GDPR is directly applicable and must not be implemented into national legislation. However, the GDPR includes certain articles that give Member States the opportunity to have specific national legislation in execution of the GDPR. This is, for instance, the case for the processing of employee personal data.

1. Has your country made use of this opportunity to have specific national rules regarding the processing of employee personal data? If so, please comment on these rules.

2. If not, has your country adopted other national data protection legislation in execution of the GDPR that could be relevant in an HR context? If so, please give a short bullet-point overview of the relevant provisions.

The GDPR contains a general prohibition on the processing of special categories of personal data and leaves it open to Member States to provide more specific rules relating to the processing of employees' personal data. The Data Protection Act 2018 (DPA 2018) which brought the GDPR into force on 25 May 2018 sets out several conditions that authorise the processing of special categories of personal data in Part 1 and Part 2 to schedule 1.

Part 1 sets out conditions relating to employment, health and research and Part 2 sets out conditions relating to substantial public interest.

Part 1 to Schedule 1 of the DPA 2018 covers:

Employment, social security and social protection. Processing is authorised if it is necessary for the purposes of performing or exercising rights or obligations imposed or conferred by law on the controller or data subject in connection with these purposes. An example could be a controller processing disability data in connection with the employment of the data subject to make reasonable adjustments. An appropriate policy document must be in place.

Health or social care. Processing is authorised where necessary for health or social care purposes. This can include occupational medicine, provision of healthcare and medical diagnosis.

Public health. Processing is authorised where necessary for reasons of public interest in the area of public health and carried out by a health professional (or under their responsibility) or another person who owes a duty of confidentiality under enactment or rule of law.

Archiving, research and statistics. Processing is authorised if necessary for archiving purposes, scientific or historical research or statistical purposes. It must be in the public interest and carried out in accordance with Article 89 of the GDPR.

Part 2 to Schedule 1 of the DPA 2018 covers the substantial public interest conditions.
There is a list of 23 conditions, which include:

- Administration of justice.
- Equality of opportunity.
- Racial and ethnic diversity at senior levels of organisations.
- Journalism in connection with unlawful acts or dishonesty or malpractice.
- Counselling.
- Occupational pensions.

In each case, more detail on application is provided in the relevant paragraph. For example, an employer may be able to collect personal data about disability, sexual orientation or ethnicity as part of the recruitment process to ensure equality of opportunity. This is if it is not used to make decisions about the data subjects or likely to cause substantial damage or substantial distress. Each is subject to the requirement to have an appropriate policy document in place.

In relation to criminal convictions and offences data, Part 3 to Schedule 1 of the DPA 2018 sets out some additional authorisations for the processing of this type of personal data not under the control of official authority (as allowed for by Article 10 of the GDPR). For this type of personal data, a controller can rely on any of the Part 1 or Part 2 conditions or one of the Part 3 conditions (section 10(5), DPA 2018). A controller still needs a lawful basis for processing under Article 6 of the GDPR.

The additional Part 3 conditions relate to:

- Consent.
- Vital interests of an individual.
- Processing by not-for-profit bodies.
- Personal data in the public domain.
- Legal claims.
- Judicial acts.
- Accounts used in the commission of indecency offences involving children.
- Insurance conditions.

In each case, more detail on its application is provided in the relevant paragraph and each is subject to the requirement to have an appropriate policy document in place.

When relying on a condition in Part 2 to Schedule 1 of the DPA 2018 for criminal convictions data, an express requirement for it to be in the substantial public interest can be disapplied if the other requirements of the condition are met (Paragraph 36, Part 3, Schedule 1, DPA 2018). There is ongoing discussion as to how these conditions could be relied on by controllers, for example to perform routine DBS (Disclosure and Barring Service) checks.

2. Does any other employment-related privacy legislation exist in your country (not necessarily in execution of the GDPR)? Has the GDPR impacted this existing privacy legislation?

There is no data privacy law in the UK which specifically governs monitoring of employees or other workers. Employers are neither expressly permitted to monitor, nor are they prohibited from doing so. Instead, as the various methods of monitoring have developed over recent years, so has the regulatory framework governing their use. The Privacy and Electronic Communications Regulations (EC Directive) Regulations 2003 (PECR) are being amended to take account of changes implemented by the GDPR. This relates to marketing calls and could have an impact in respect of recruitment agencies. The most recent updates came into effect on 8 September 2018, with some updates to cover changes made by the GDPR from 25 May 2018.

The Regulation of Investigatory Powers Act 2000 (RIPA 2000) and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699) (Telecommunications Regulations 2000) apply where electronic communications are intercepted during transmission. In 2018, relevant sections of RIPA 2000 are due to be replaced by provisions in the Investigatory Powers Act 2016 and the Telecommunications Regulations 2000 are due to be replaced by the Investigatory Powers (Interception by Businesses etc. for Monitoring and Record-keeping Purposes) Regulations 2018 (SI 2018/356).

Article 8 of the European Convention on Human Rights (the "ECHR" as incorporated into UK law by the Human Rights Act 1998 ("HRA") provides individuals with the right to respect for private and family life and correspondence including in the workplace but this is generally confined to where there is a reasonable expectation of privacy.

The duty of trust and confidence implied into an employee's contract of employment is also relevant as the employer's monitoring activities may constitute a breach of this duty, depending on the circumstances.

3. The information obligation of employers (data controllers) towards their employees has been extended under the GDPR. Therefore, the current information clauses/policies will probably no longer be sufficient.

1. By what means (e.g. (an annex to) the employment contract, work rules, a policy) would you recommend employers in your country provide employees with this extended information?

2. Should any particular procedure be complied with?

One of the key themes under the GDPR is transparency. Employers should notify their staff with extended information by providing revised policies to staff along with detailed information on where information relating to data protection can be found within the business. In this context employers are best advised to issue privacy notices to all employees. Common pitfalls can often be holding unnecessary personal data or retaining personal data beyond a reasonable time frame. Below are the points that should be covered off when updating a privacy notice in order to be GDPR compliant:

- The organisation's identity and contact details;
- Details of the Data Protection Officer (if applicable);
- The purpose of processing;
- The legal basis for processing;
- The organisation's legitimate interests if applicable;
- Who will be receiving personal data;
- Whether the data will be transferred outside the EEA;
- Retention periods and information on storage processes;
- Whether automated decision making is in use;
- Consequences of the individual not providing personal data and whether the individual is required by contract, law or another reason;
- Data subject rights ie erasure, rectification;
- Any changes necessary to ensure ongoing compliance.

4. Is 'consent of the employee' used as a legal justification ground to process his/her data in your country, required/advised/discouraged? Can you illustrate with some examples?

Employee consent used to be considered the safest option, however the Information Commissioners Office (ICO) (the UK GDPR enforcement agency) has suggested that the extent to which consent can be relied upon in the context of employment is "limited" given the unequal position of an employment relationship could suggest consent has not been freely give as required under the GDPR.

Employers should not, in most situation, use consent as a lawful basis for processing and should look for another legitimate basis for processing, such as the processing is necessary in order to perform the contract. For example an employer would be unable to pay an employee, or provide them with other provisions within a contract without processing personal data.

Employers could also rely on the requirement to comply with a legal obligation to process personal data, for example providing details to a governing body such as HMRC (the UK tax authority).

A client of ours recently wanted to film its staff for a promotional video for perspective clients and the general public. In this situation we advised that consent was appropriate as it could be freely given and was not conditional upon their employment.

It is envisaged that employers are more likely to remove any standard consent clauses within employment contracts and instead highlight in the contract that any processing of data will be in accordance with a separate privacy notice.

5. The GDPR provides that a DPO benefits from dismissal protection. However, the GDPR does not provide for any penalties for the employer in case of any violation of this dismissal protection.

Can an employer in your country be sanctioned for dismissing a DPO for reasons related to his/her tasks as DPO? If yes, on what basis and what will be the penalty/ies?

A Data Protection Officer (DPO) must be involved in all issues which relate to the protection of personal data. The tasks of a DPO are set out in s.71 DPA 2018 as follows:

As a result, DPOs are offered protection against dismissal for reasons relating to its performance of DPO tasks. For example, if the DPO comes to a conclusion that processing of personal data is high risk and a data protection impact assessment is required or, for example, it suggests changes to the employer's policies which the employer does not agree with, then the DPO cannot be dismissed for giving this advice. Dismissing a DPO for decisions they make will result in a breach of both the GDPR and the DPA 2018. The DPA 2018 states that the penalty for an infringement of Article 70 is the standard maximum amount being:

- in the case of an undertaking, 10 million Euros or 2% of the undertaking's total annual worldwide turnover in the preceding financial year, whichever is higher, or
- in any other case, 10 million Euros.

The DPO, as an employee would be able to claim unfair dismissal. The maximum amount that you can be awarded as compensation for Unfair Dismissal is presently the statutory cap of £83,682, or 52 weeks gross salary- whichever is the lower. This is in addition to the basic award which can be ordered by the Tribunal of up to a maximum of £15,240.

6. What legal action(s) can an employee take against an employer in your country if he/she believes that his/her data protection rights are not being respected?

An employee is entitled to make a data subject access request to establish what personal data the employer holds. It is advised that they write to their employer requesting exactly what personal data they would like to receive, as a data subject may not need to see absolutely everything that is held by an employer. An employer has one month in which to respond to a data subject access request. If an employee is dissatisfied with the outcome of a data subject access request, then they can make a complaint to the ICO.

Under the GDPR and DPA 2018 an employee may take legal action in order to achieve the following rights:

- to be informed if their personal data is being used;
- to obtain copies of their data;
- to have their data rectified;
- to have their data deleted;
- to limit how the employer uses their data;
- to data portability (ie. to receive information in an accessible way);
- to object to use of personal data; and
- to prevent automated processing unless exceptions apply which are that it is necessary for the purposes of a contract, it is authorised by law or is based on explicit consent.

Ordinarily you would expect the employee to contact the employer in the first instance. If they don't receive a satisfactory response, they can also make a complaint to the ICO.

An employee may also wish to seek to enforce their rights through legal action in the courts. Any employee who has suffered material or non-material damage as a result of an infringement of the GDPR has the right to receive compensation from the controller for the damage suffered. Damage includes financial loss, distress and "other adverse effects".

7. Does your national legislation fix a storage period for HR-related documents?

There is no set storage period for HR related documents in the UK. The GDPR states that businesses should retain personal data for no longer than is necessary for the purposes for which it is processed. This does not however rule out holding personal data to protect against legal risk. In the absence of statutory requirement, a risk based approach has been taken to retention periods in the UK.

Some employment documents may, for example, be kept for 7 years as they could be relevant to a tribunal, County Court or High Court claim. This takes into consideration the 6 year limitation period in the UK plus a further year for any potential claims to be brought to the employer's attention.

Employers should continue to take a risk based approach, and consider what data they should keep and for what periods of time. For example, it is rare that there would be a need to retain the current bank account details of an employee who is no longer with the business. In contrast, PAYE records should be kept for longer in case of any investigations by HMRC.

In a recruitment exercise you might consider holding certain documents for a shorter period of time which covers the possibility of, for example, discrimination claims which generally need to be brought within 3 months of the discriminatory act.

The ICO has released some guidance in relation to certain scenarios. For example, any information retained from a recruitment exercise should only be retained for a maximum of 6 months, and in any event, should be destroyed as soon as possible.

8. The GDPR obliges each country's supervisory data protection authority to draw up a list of the kinds of processing operations that, in its view, require a Data Protection Impact Assessment ('DPIA'), i.e. the controller's assessment of the impact of the envisaged processing operations on the protection of personal data where a type of processing is likely to result in a high risk. The supervisory data protection authority may also (but is not obliged to) draw up a list of the kinds of processing operations for which no DPIA is required.

1. Has your country's supervisory data protection authority only established a list of processing operations that require a DPIA or also a list of processing operations that do not require a DPIA?

2. Do any of these lists include HR-related processing operations?

In addition to the examples provided under Article 35(3) of the GDPR in respect of the types of processing that automatically require a DPIA, the ICO has published a list under Article 35(4) setting out ten more:

- Innovative technology;
- Denial of service;
- Biometric data
- Genetic data;
- Data matching;
- Invisible processing;
- Tracking;
- Targeting of children/other vulnerable individuals for marketing, profiling for auto decision making or the offer of online services; and
- Risk of physical harm.

One concern for employers out of the above would be any biometric data that is used for example, in work place access systems or identity verification. Tracking should also be considered by employers, particularly if they are using this to process location data of employees. Finally, risk of physical harm could come into the remit for HR departments in circumstances such as where processing of data is used in connection with a whistleblowing complaint and as such, a personal data breach could jeopardise the safety of a data subject.

The ICO has not established a list of processing operations that do not require a DPIA.

9. Has your country's supervisory data protection authority given any employment law-related advice or made any recommendations since the GDPR has entered into force?

The ICO has not yet updated its guidance for employers to reflect the GDPR and Data Protection Act 2010 and will do so in due course.

The ICO has, however, issued general guidance which has application in an employment contest such as:

- A Guide to the General Data Protection Regulation (GDPR). This is described as a "living document" which is frequently added to by the ICO.

- Preparing for the General Data Protection Regulation (GDPR): 12 steps to take now.

10. 1. Are there in your country any additional conditions, on top of what is provided for within the GDPR, to process any special categories of personal data? If so, which conditions and for which type(s) of data do they apply?

2. Does your national legislation authorize the processing of personal data relating to criminal convictions and offences? If so, when is this authorized and what are the appropriate safeguards that should be complied with (if any)?

There are ten conditions for processing special category data in the GDPR itself, but the DPA 2018 introduces additional conditions and safeguards. The DPA implements derogations which allows the processing of special categories of personal data and criminal conviction data where a justification exists. s.11 DPA 2018 makes supplementary provisions relating to the processing of special categories of data and personal data relating to criminal convictions and offences.

If an employer is processing special category data, then the employer needs to have a policy document in place detailing how it does this. The employer also needs to observe additional safeguards which include retaining the policy document and always keeping records of any conditions for the processing.

Section 11(2) of the DPA 2018 provides that criminal convictions data includes personal data relating to the alleged commission of offences by the data subject, proceedings for the offence and disposal of such proceedings including sentencing.

The processing of personal data relating to criminal convictions and offences or related security measures is authorised by UK law for the purposes of Article 10 only if the processing meets a condition and safeguard in Part 1 (conditions relating to employment, health and research etc), Part 2 (public interest conditions) or Part 3 (conditions relating to criminal convictions) of Schedule 1 to the DPA 2018.

An employer can process personal data relating to criminal convictions and offences or related security measures if the processing is "necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller or the data subject in connection with employment". Additional safeguards concern both the retention of the policy document and the employer maintaining a record of the condition it relied on to undertake the processing. All official criminal record checks are performed via the Disclosure and Barring Service and this recommends retaining such documentation for a maximum period of 6 months – this is subject to any relevant regulatory provisions which might request a longer period.

NOTES