GDPR Hot Topics – Employer Essentials

November 15, 2018

Mandy Perry, Partner – UK
André Zimmermann, Partner – Germany
Hélène Daher, Partner – Paris
Mario Scofferi, Of Counsel – Italy

orrick

United Kingdom

Mandy Perry

orrick

GDPR/Data Protection Act Overview – Definitions

The **GDPR** and the Data Protection Act in the UK regulates the "**processing**" of "**[sensitive] personal data**"

"personal data"

- Any **information** relating to an **identified** or **identifiable individual.**

"sensitive personal data"

- Special category of personal data, defined as information concerning and individual's:
  - ✓ **Race** or **ethnicity**
  - ✓ **Political opinions**
  - ✓ **Religious** or other **philosophical beliefs**
  - ✓ **Trade union membership**
  - ✓ **Physical** or **mental health information**
  - ✓ **Sexual preferences**
  - ✓ **Genetic** or **biometric data**

"processing"

- Essentially this means **using the personal data** in **any way**.
- Such as "collecting; recording; organising; structuring; storing; adapting or altering; retrieving; consulting; **using**; disclosing by transmission, dissemination or otherwise making available; aligning or combining; restricting; erasing; or destroying".

Principles of Processing Personal Data

Lawfulness, fairness & transparency	✓ Personal data shall be *processed lawfully, fairly and in a transparent manner.*
Purpose limitation	✓ Personal data shall be *collected for specified, explicit and legitimate purposes.*
Data minimisation	✓ Personal data shall be *adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.*
Accuracy	✓ Personal data shall be *accurate and, where necessary, kept up to date.*
Storage limitation	✓ Personal data shall be *kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.*
Integrity & confidentiality	✓ Personal data shall be *processed in a manner that ensures appropriate security of the persona data, including protection against data breaches.*
Accountability	✓ The controller shall be responsible for, and able to demonstrate compliance with, the above principles.

Data Subject Access Requests

Data Subject Access Requests

- The GDPR provides for new and enhanced rights for individuals in relation to their personal data:
  - **Right of access**. The right to receive a copy of their Personal Data and to obtain various details about the processing;
  - **Right to data portability**. The right to receive their personal data in a structured, commonly-used and machine readable format and have the right to transmit that information to another data controller.
  - **Right to rectification**. The right to obtain rectification of their personal data without undue delay where that personal data is inaccurate or incomplete.
  - **Right to erasure**. The right to obtain the erasure of their Personal Data without undue delay in certain circumstances, such as where the Personal Data is no longer necessary in relation to the purposes for which it was collected or processed.
  - **Right to restriction**. The right to obtain the restriction of the processing undertaken by the company on their Personal Data in certain circumstances, such as where the accuracy of the Personal Data is contested by the Team Member, for a period enabling the company to verify the accuracy of that Personal Data.
- These rights apply only in certain circumstances and there are also various exemptions.
- ICO complaints and responses

Consent

The GDPR sets a high standard for consent. It must:

- Be unambiguous, involve a clear affirmative action (an opt-in), provide distinct ('granular') consent options for distinct processing operations, be capable of being withdrawn and be freely given.
- Employers must keep clear records to demonstrate consent.
- The GDPR gives a specific right to withdraw consent. Employers need to tell employees about their right to withdraw, and offer them easy ways to withdraw consent at any time. This should also be well documented.
- Employers should review existing consents and consent mechanisms to check they meet the high GDPR standard.

Background Checks

- Depends on what you are checking and why – relevant and necessary for the role
- Criminal records – DBS system - spent and unspent convictions
- Requiring the employee to obtain criminal record by subject access request is criminal offence under Section 184 of the Data Protection Act 2018
- Third party vendors

Germany

André Zimmermann

orrick

Germany (1/5)

- **May the works council denigrate the employer to the data protection authorities?**
  - Principle of trustful cooperation
  - Only after prior reporting to employer and DPO?

Germany (2/5)

- **Will employees claim damages for data breaches?**
  - So far only damages granted in the event of a serious violation of the right of personality
  - Now sufficient that immaterial damage has occurred
  - Labor courts will likely grant higher immaterial damages than pre-GDPR

Germany (3/5)

- **What should be done if employees assert claims to information?**
  - Employees increasingly asserting claims for information
  - Right of access to personal data which are processed by the employer
  - Comprehensive catalogue of information that employer must provide
  - Information to be provided without delay and generally within one month
  - Be prepared!

Germany (4/5)

- **When must employee data be deleted?**
  - Delete personal data without delay where they are no longer necessary for the purposes for which they were collected or otherwise processed
  - During the ongoing employment relationship, but especially after end of employment
  - Part of a company-wide deletion concept that captures all types of data
  - Statutory provisions
  - Statute of limitations

Germany (5/5)

- **What must be taken into account when drawing up shop agreements?**
  - Shop agreements can be legal basis for processing of employee data
  - Specific requirements, i.a. include provisions on the fundamental rights of data subjects and the transparency of processing
  - Need to adapt "old" works agreements
  - Transparency and intended purpose of processing

France

Hélène Daher

A New Complex Legal Framework

In France, the GDPR's entry into force substantially **complexified** the legal framework employers have to comply with :

Before the GDPR

Law n° 78-17 of 6 January 1978 on information technology, data files and civil liberties

After the GDPR

Law n° 78-17 of 6 January 1978 as amended by Law n° 2018-493 of 20 June 2018
+
GDPR

An ***ordinance*** aiming at harmonizing/simplifying this legal framework is expected by the end of 2018/early 2019

A New Global Approach

Reinforcement of the CNIL's powers (French Supervisory Authority)

CNIL
COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

The CNIL is the ***Independent Supervisory Authority*** **responsible for monitoring the application of this GDPR**. Its powers have been increased, and now may notably fine employers for way higher amounts :

Before **2016**	After the 2016 reform (anticipation of the GDPR)	After the GDPR
€150.000 maximum fine (in practice, employers rarely received fines over € 10.000)	€3.000.000 maximum fine	€10.000.000 / €20.000.000 or 2% / 4% of the company's annnual worldwide turnover maximum fine

Strengthened Protections for the Employees' Personal Data

New protections deriving from the GDPR, notably :

- Extension of the right to **data portability** (previously limited to consumer law);
- An emphasize on the employee's consent to **personal data processing**;
- A broader **information of** the employees.

These new protections are already producing new trends in litigation

Employees may Obtain Damages through Union-led Class Actions

New possibility for employees to obtain **damages** though **union-led class actions**

The impact that this new tool will have is difficult to assess, as class actions are new in the French legal system

2014	2016	After the GDPR
First class action in the French legal system (consumer law)	First Employment law class actions: Discrimination class action & class action to put an end to a data protection violation (no damages possible)	Class action aiming at putting an end to a data protection violation and asking damages

Areas that may not be Strongly Impacted by the GDPR

1
Background checks, hiring processes

2
Role of staff representative bodies

3
Maximum retention periods

Italy

Mario Scofferi

orrick

The new Italian Privacy Code (Legislative Decree no. 196/2003) as modified and implemented by the Legislative Decree no. 101/2018: main provisions

In general	In the context of the employment relationship
• Adjustment of the Italian rules according to the provisions of the GDPR (artt. 1 and 2) • the reference to laws and regulations as a legal basis and a prerequisite for the lawfulness of processing «*for the performance of a task carried out in the public interest or in the exercise of official authority*» (art. 2-*ter*) • the future promotion of ethical rules by the Italian Privacy Authority (art. 2-*quater*) • definition of all cases of major public interest for which the processing of special categories of personal data is necessary (art. 2-*sexies*) • the Italian Privacy Authority shall issue a measure (every two years) setting out the relevant guarantee measures for the processing of genetic, biometric and health data (art. 2-septies)	• the Italian Privacy Authority will promote the adoption of ethical rules concerning the employment relationship (art. 111 of the Legislative Decree no. 196/2003) • the information set forth by art. 13 of GDPR, in case of receipt of *curricula* sent by workers, shall be given at the moment of the first contact with such worker after the resume has been sent; and in such case the consent to personal data treatment will not result necessary (art. 111-bis)

In general	In the context of the employment relationship
• principles with regard to the processing of data relating to criminal convictions and offences (art. 2-octies) • limitations of the rights of data access (art. 2-*undecies*) • arrangements for lodging a complaint, in addition to the one to the Italian Privacy Authority, to the ordinary judicial authority (art. 13) • the provision for new offences (art. 15) • the handling of previously submitted business, only if declared topical (art. 19) • previous ethical and good conduct codes set forth by the previous Italian Privacy Code will still be in force for 1 year (art. 20) • the general authorizations released by the Italian Privacy Authority still remain in force for a transitional period of 150 days (art. 21) • for the first 8 months after Legislative Decree no. 101/2018 is effective, in applying administrative sanctions the Italian Privacy Authority will take into account «*the first phase of application of the sanctioning provisions*» (art. 22)	• application of art. 8 of the Italian Statute of Employees to Data collection (art. 113 of Legislative Decree no. 196/2003) • application of Article 4 of the Italian Statute of Employees with regard to remote control (art. 114 of Legislative Decree no. 196/2003) • obligation to guarantee, in cases of remote work, the respect for the personality and moral freedom of the worker (art. 115 of Legislative Decree no. 196/2003)

Employer Essentials: The Consent

No need for consent for the processing of personal data of the employee, to the extent that at least one of the conditions pursuant to art. 6 of the GDPR applies and, in particular:

letter b): «*processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract*»

No need for consent for the processing of «special categories» of personal data of the employee, to the extent that at least one of the conditions pursuant to art. 9 of the GDPR applies and, in particular:

b): «*processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law*»

c): «*processing is necessary to protect the vital interests of the data subject or of another natural person*»

f): «*processing is necessary for the establishment, exercise or defense of legal claims*»

g): «*processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law*»

h): «*processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee*»

…the consent in relation to data relating to criminal convictions and offences

No need for consent for the processing of data relating to criminal convictions and offences, to the extent that at least one of the conditions pursuant to art. 6 of the GDPR applies, but a specific rule at art. 10 of the GDPR, is provided

«*Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects*»

art. 2–*octies* of the Legislative Decree n. 196/2003 (as implemented by the Legislative Decree n. 101/2018), maintaining the conditions for use set out in art. 10, GDPR, provides that the processing of such data is allowed only if authorized by a law or regulation or, failing that, by a decree issued by the Ministry of Justice: until the adoption of the latter, the processing of the data in question is authorized only if in implementation of memoranda of understanding for the prevention and combating phenomena of organized crime stipulated with the Ministry of the Interior or with the prefectures - UTG, subject to the opinion of the Italian Privacy Authority

Employer Essentials: Background Checks

Art. 113 of the Legislative Decree no. 196/2003, in relation to data collection and relevance of them, provides for the application of art. 8 of the Italian Statute of Employees

Art. 8 of the Italian Statute of Employees

«*For the purposes of recruitment, as in the course of the employment relationship, the employer is prohibited from carrying out investigations, including through third parties, on the political, religious or trade union opinions of the worker, as well as on facts that are not relevant for the purposes of assessing the worker's professional aptitude*»

The Italian case-law

According to the Italian case-law, infringement of Article 8 occurs whenever investigations are based on opinions or facts which do not serve to assess the worker's professional abilities

The rulings of the Italian Privacy Authority

Also the Italian Privacy Authority has repeatedly stressed the need to ensure compliance with Article 8 as regards investigations and aptitude tests prior to the recruitment phase

Employer Essentials: Access Request

Art. 15 of the GDPR

«*The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data…*»

More information than before

«*…and the following information*», including:

letter c): «*the recipients or categories of recipient to whom the personal data have been or will be disclosed*»

letter d): «*where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period*»

par. 2: «*Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer*»

Moreover, pursuant to Artt. 13 and 14 of the GDPR, the controller shall provide the data subject with some information on the processing of data and, among others, «*the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability*»

Employer Essentials: Cross-Border Transfer (to *extra* UE countries)

Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if the conditions laid down in Chapter V of the GDPR are met

1. In case a country has an adequate level of protection, the transfer shall not require any specific authorization (art. 44 of the GDPR)
2. Otherwise, the European Commission shall asses the adequacy of the level of protection of the country (art. 45 of the GDPR) or the presence of adequate safeguards provided by the controller or the processor (art. 46 of the GDPR)
3. In absence of the latter, derogations for specific situations are provided (art. 49 of the GDPR)

Usually:

- contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organization **(standard data protection clauses)**; or
- **binding corporate rules** in accordance with Article 47 of the GDPR

orrick