GDPR AND EMPLOYMENT LAW

JEFFREY KENENS

GGI EUROPEAN CONFERENCE

BERLIN, 20 APRIL 2018

TeekensKarstens
advocaten notarissen

WHAT WORDS COME TO MIND WHEN YOU THINK ABOUT PRIVACY?

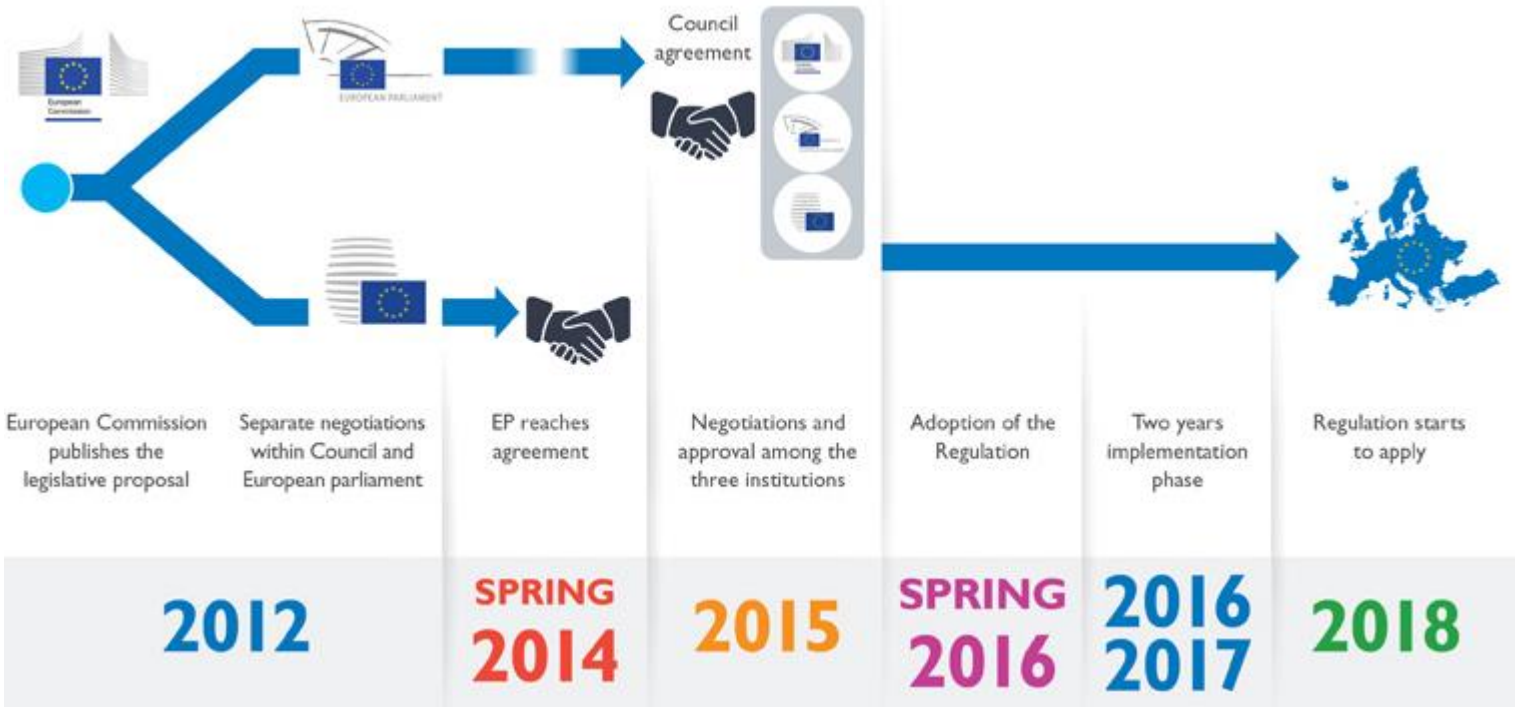
FEW MORE WEEKS UNTILL THE GDPR

- Previous legislation: Data Protection Directive (1995)
  Outdated → updated by GDPR

- **Article 29 Working Party**
  - Advisory body
  - Made up of a representative from the Data Protection Authority of each EU Member State, the European Data Protection Supervisor and the European Commission
  - Publishes guidelines that clarify various GDPR-terms

  http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358

FEW MORE WEEKS UNTILL THE GDPR



FEW MORE WEEKS UNTILL THE GDPR

GDPR in short

- Scope legislation: any company either based in EU or which deals with data involving EU citizens or organizations (no matter where company is based)
- Scope personal data: personal data includes anything that might identify an EU citizen
- High fines in case of breaches

FEW MORE WEEKS UNTILL THE GDPR

GDPR in short

- Personal data must be:
  - Processed **lawfully**, fairly and transparantly.
  - Be adequate, relevant and **limited** to what is necessary for processing.
  - **Accurate** en kept up to date.
  - Kept in a form such that the data subject can be identified only as long as is **necessary** for processing.
  - Processed in a manner that ensures its **security.**
  - and can only be collected for specified, explicit and legitimate **purposes.**

WHAT DATA QUALIFIES AS ‘PERSONAL DATA’?

PERSONAL DATA

For instance:

- name and address details
- date of birth, emailaddress, telephone number
- IBAN details
- salary data
- sickness absence registration
- camera footage
- number plate, tracking- or location data
- CV, letter of application, certificates

LAWFULNESS OF PROCESSING

Processing of personal data shall be lawful only if one of the six principles of article 6 GDPR is applicable. The processing:

1. **is necessary to prepare or carry out a contract with the data subject (e.g. contract of employment);**
2. **is necessary to comply with a legal obligation;**
3. is necessary in order to protect the vital interests of the data subject;
4. is necessary for the performance of a task carried out in the public interest;
5. **is necessary for the purposes of the legitimate interests pursued by the controller or by a third party;**
6. **has been approved by the data subject (consent).**

CONSENT

You place job vacancies on your website containing the following notice:

"*By uploading your personal data you are giving your consent to Company X to process your uploaded data. Company X processes the data by reason of the provided consent.*"

GROUND FOR PROCESSING DATA: CONSENT

Valid consent has to fulfill the following conditions:

- Given in freedom: option to refuse without negative consequences (NB: not assumed quickly in an employment relationship);
- Specific and informed: in an understandable and easily accessible way; provide clarity in a clear and simple manner about the purpose of processing, third parties, retention periods;
- Unambiguous: there is no doubt about the provided consent (opt in/opt out)

GROUND FOR PROCESSING DATA: CONSENT

- Consent has to be granted per processing purpose;
- Burden of proof is on the controller;
- The data subject has to be notified (before granting the consent) that the consent can be revoked at any time;
- Consent does (generally) not repair an 'unfair' processing of personal data.

JOB APPLICATION

Is an employer (in principle) allowed to ‘google’ an applicant and view his Facebook- and Instagramaccount?

JOB APPLICATION

No, this is only allowed when the employer has a legal ground to process the applicants' data that are on the internet.

E.g. when the information is of major interest for the position. The job applicant has to be notified and given the chance to explain and comment on the found information.

JOB APPLICATION

Is an employer allowed to demand job applicants to apply via video?

JOB APPLICATION

No, this is not allowed.

Applying by video can imply the processing of specific personal data, like information about human race, religion (clothing) and health (visible handicap).

These personal data can only be processed with **explicit consent** from the job applicant. The consent is only valid if the job applicant has a free choice and it is apparent that his choice does not have a negative impact.

JOB APPLICATION

Is an employer allowed to request a copy of the job applicant's ID during the application?

JOB APPLICATION

No, this is not allowed.

A copy of an ID contains data that are not necessary for the employer during the application procedure.

However, the employer is allowed to verify the identity of the applicant, by inspecting the ID.

Does the applicant enter the employment with the employer? Then the employer is legally obliged to have a copy of the ID.

JOB APPLICATION

You store data of job applicants (letter of application, CV, notes, results of assessments) for two years in your HR-systems.

Is this allowed?

JOB APPLICATION

No.

The GDPR does not contain retention periods.

However, article 5.1e states that the period during which personal data may be stored, ends when the personal data are no longer needed.

CONTROLLING EMPLOYEES: LEGAL FRAMEWORK

- Processing has to be based on one of the six legal bases: **legitimate interest** (legitimate purpose that outweighs the privacy interests of the employee, e.g. protecting business secrets, checking compliance).

- **Proportionality and subsidiarity**: the purpose can not be achieved in a less far reaching manner.

- **Recognisability**: employer informs employees in advance with regards to what is allowed/forbidden, that verification is possible and how this takes place.

NL: prior consent of the works council.

CONTROLLING EMPLOYEES: LEGAL FRAMEWORK

Additional requirements when controlling covertly:

- Reasonable suspiscion of a criminal offence or prohibited behaviour.
- Has to be part of a range of measures.
- Employee requests investigation at supervisory authority to check if intended covert investigation is allowed.
- Employer informs the involved employee afterwards, also when the suspicion proves to be unjustified.

CONTROL: SICK EMPLOYEES

Article 9 GDPR: processing data regarding health is prohibited

Exception on prohibition, article 9 second paragraph sub b and sub h GDPR:

for carrying out obligations of the controller in the field of employment and social security and for the assessment of the working capacity of the employee, medical diagnosis, provision of health or social care.

CONTROL: SICK EMPLOYEE

What data is an employer allowed to request when the employee calls in sick?

CONTROL: SICK EMPLOYEE

- Telephone number and address where employee is treated
- Date first absence day
- Date of (partial) recovery
- Probable duration absence
- Current assignments and operations
- Whether a safety net provision or possibility of recourse exists
- Whether the sickness is related to a workplace accident

PERSONNEL FILES

Is the employee entitled to a copy of his personnel file?

PERSONNEL FILES

Yes.

Conditions for building personnel files. Employers:

- Are responsible for accuracy of data.
- Are not allowed to document more data than needed and the data should be relevant.
- Must secure the data.
- May not store data longer than needed.

PERSONNEL FILES

Are data concerning human race, sexual orientation, belief, political preferences and health information allowed to be stated in the personnel file?

PERSONNEL FILES

No, in principle not.

These types of data are qualified as '*special personal data*' under article 9 GDPR.

PERSONNEL FILES

Does the managing director of a company in principle have access to the personnel files?

PERSONNEL FILES

Yes, but only in so far as this is necessary for doing his job (control of employee his performance/ realizing targets).

PERSONNEL FILES

Does the GDPR contain a specific retention period for personnel files?

PERSONNEL FILES

The GDPR does not contain retention periods.

However, article 5.1 states that the period during which personal data may be stored, ends when the personal data are no longer needed. When the data are no longer necessary, the data have to be destroyed.

DATA PROTECTION OFFICER

Is every employer obliged to appoint a Data Protection Officer?

DATA PROTECTION OFFICER

No.

This is only obligatory for:

- government bodies;
- organisations that (on a large scale) observe individuals, and;
- organisations that (on a large scale) process special personal data (hospitals, corporate investigations).

DATA BREACHES

- Data breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

- So, not only the 'leaking' of data, but also wrongful processing of data.

- E.g. stolen laptop or telephone, lost USB-stick, break-in by hacker in data files, email with personal data sent to the wrong recipient.

DATA BREACHES

- Report to the supervisory authority, unless it is not probable that the data breach is a risk for the rights and freedoms of natural persons.

- Report to the natural person when there is a probable high risk concerning his rights and freedoms.

Policy art. 29 Working Party can be of help (when considering the risks).

Violation of the obligation to report data breaches to the supervisory authority → supervisory authority can impose a fine of 10 million euros maximum, or 2% of the worldwide annual turnover (in case this is more).

DATA BREACHES

How much time are you allowed to take before reporting a breach?

24, 36 or 72 hours?

DATA BREACHES

Within 72 hours of becoming aware of the breach → report to the supervisory authority.

Not possible? Motivate the delay.

FIVE PRIORITIES

1. Awareness and compliance choices (inform employees about the GDPR and make choices)
2. Baseline measurement
   - ✓Analyse business processes and processing of personal data;
   - ✓What processors do you have? Who receives personal data and for what purpose?
   - ✓Start with a process register!
3. Processing agreement
4. Data leak protocol and data breach register
5. Privacy Statement and Privacy Policy (employee manual!)

LOCATIONS TEEKENSKARSTENS

LEIDEN

Vondellaan 51
P.O. Box 201
2300 AE Leiden
T +31 71 - 535 81 30
F +31 71 - 535 80 01
E info@tk.nl

ALPHEN AAN DEN RIJN

Prins Bernhardlaan 4
P.O. Box 402
2400 AK Alphen aan den Rijn
T +31 172 - 41 98 44
F +31 172 - 43 42 51
E info@tk.nl

WWW.TK.NL