DON’T MESS WITH PERSONAL DATA

LEXIA
Legal Excellence

AGENDA

1. Key elements in data protection compliance

2. Recent case law and new guidelines: things to learn?

3. Data transfers to outside the EU: what is going on?

KEY DATA PROTECTION REGULATION

General Data Protection Regulation (EU 2016/679) (GDPR)
ePrivacy Directive (2002/58/EC)

- **Data Protection Act**
- **Act on Electronic Communication Services**
- **Act on the Protection of Privacy in Working Life**
- **Sector specific legislation**

PRINCIPLES RELATED TO PROCESSING

Be complied with the processing rules

1. Lawfulness, fairness, transparency
2. Purpose limitation
3. Minimisation of data

Able to **demonstrate** compliance / accountability

4. Accuracy of data
5. Storage limitation
6. Confidentiality and security

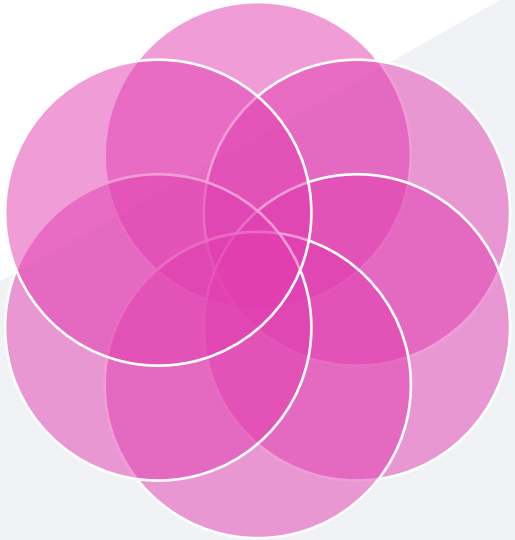
LEGAL BASIS FOR PROCESSING

Determine in advance
Remember the accountability

Consent

Contract

Legitimate interest



Excercise of public authority

Legal obligation

Protection of vital interests

PROCESSING OF HEALTH DATA

- Personal data concerning a **health status of data subject** is included in **special categories of personal data** of the GDPR (i.e., sensitive personal data)
- **What is health data?**
  - **Broad definition**: Health data includes information on a person's physical and mental health or information on the use of health care services (if the data reveal a person's health status).
    - For example: if an app collects certain physical information such as hearth rate and speed of a user during a sport activity, and combine this data to other personal data, and analyze the data medically, as an outcome the data might include data concerning a health status of the user.
- As a rule, under the GDPR, processing of health data is **prohibited**...
  - Unless there is a **specific legal ground for the processing**.
- Legal ground must be based on the GDPR or other applicable legislation.
  - Legal grounds stipulated in the GDPR: a **consent** among others.
  - Other legal grounds can be found out, for example, in employment laws or patient legislation.
- Consent must be **explicit**, and it’s not allowed to include consent terms in privacy policies or terms and conditions.
  - Contract or legitimate interest is rarely a valid legal basis to process health data.

DOCUMENTATION AND ACCOUNTABILITY

HOW TO DEMOSTRATE COMPLIANCE WITH THE GDPR?

→ DOCUMENTED, DOCUMENT AND DOCUMENT…

- DATA MAPPING AND DATA FLOWS
- EXTERNAL PRIVACY POLICIES AND NOTICES
- DPAs, JOINT-CONTROLLERSHIP AGREEMENTS AND DATA SHARING AGREEMENTS
- DATA PROTECTION AND SECURITY POLICIES, INTERNAL GUIDELINES FOR STAFF AND OTHER STAKEHOLDERS
- RECORDS OF PROCESSING ACTIVITIES
- RISK ASSESSMENTS AND DATA PROTECTION IMPACT ASSESSMENTS (DPIA)
- DEFINE THE ROLE OF DPO AND DATA PROTECTION ORGANIZATION AND DOCUMENT ACTIVITIES

RECENT CASE LAW: THINGS TO LEARN?

LEXIA
Legal Excellence

RECENT CASE LAW

- More than 120 000 data breach notifications have been investigated by the EEA supervisory authorities in 2020.

- Altogether more than 550 GDPR administrative fines within the EEA since 2018.
  - Sanctions under the GDPR more than 150 million euros in 2020.
  - The largest recent administrative fines: Google € 50 million, H&M €35 million, British Airways €22 million, Marriott €20.4 million.

- Finnish data protection authority has imposed administrative fines around ten times. In addition, other corrective measures have been imposed such as obligation to delete certain personal data or stop processing.

CASE 1 – INFORMING DATA SUBJECTS AND TRANSPARENCY OF PROCESSING

- The company **had not appropriately informed data subjects** of their rights under data protection legislation.
- Data subjects were, among other things, not informed about the right to object the company to disclose personal data to third parties for direct marketing purposes.
- **The right to object to the processing for direct marketing** was notified only to those data subjects who had purchased additional services.
- The company was considered to have **failed to comply with the principle of transparency** and **information obligations under the GDPR**.
- The violation affected 161,000 customers during 2019 alone.
- The amount of administrative fine was EUR 100,000.

CASE 2 – DPIA

- The company **had processed a location data of its employees** by tracking vehicles.
  - Location data was mainly used to monitor working hours.
- The case was considered to be about a systematic monitoring of location data. In addition, according to the authority, there was an imbalance of power between the employees (data subjects) and the employer (controller).
- **A data protection impact assessment (DPIA) shall be carried out**, for example, prior to the processing of location data, where location data is used for systematic monitoring, and the processing is directed towards data subjects who are at a disadvantage compared to the controller.
  - **The company had not carried out a DPIA before starting to process the location data**.
- The amount of administrative fine was EUR 16,000.

CASE 3 - COLLECTING OF UNNECESSARY PERSONAL DATA

- The company had processed personal data **in violation of key provisions of the Act on the Protection of Privacy in Working Life**, and there **was no legal basis for processing personal data**.
- The company collected personal data about employees using a form, on the employee's religious beliefs, health status, possible pregnancy, and family relationships.
  - Such personal data constitutes data to be considered in specific categories of personal data under the GDPR, and the processing is only permitted under the valid legal basis.
- In addition, a **violation of the principle of minimization of data** and **shortcomings in privacy documentation**.
- The company was unable to demonstrate its compliance with law when processing personal data of employees and job applicants.
  - The Data Protection Authority (DPA) ordered the company to delete unnecessary personal data and ordered to complete the documentation.
  - In addition, an administrative fine of EUR 12,500.

CASE 4 – ELECTRONIC DIRECT MARKETING AND RIGHTS OF THE DATA SUBJECT

- The company **had sent electronic direct marketing messages without a prior consent**.
  - As a main rule under the Act on Electronic Communication Services, electronic direct marketing for private persons needs a prior consent.
- In addition, **the company had failed to comply with the rights of the data subject**.
  - The company had not responded to or implemented requests for the rights of the data subjects, and the company was unable to demonstrate that it had processed personal data lawfully.
    - Some of the recipients had asked for direct marketing to be stopped, but they had received marketing messages despite the marketing bans.
- Administrative fine of EUR 7000.

CASE 5 – CONSENT TO THE USE OF COOKIES

- **The company did not ask a consent for a use of cookies**, but the company informed users on the use of cookies through a cookie banner on its website. Cookies were used for personalization and targeting advertising among others.
- According to DPA, **a consent for a use of cookies must be asked in accordance with the GDPR requirements.**
- It cannot be considered a valid consent that a users were informed of the possibility of banning the storage and use of cookies from browser settings.
- **Consent must be an active, explicit and informed measure**.
  - Consent can be given in a variety of ways but cannot be given by silence or pre-ticked boxes.
  - User must have the opportunity to choose whether to accept or reject the cookies.
- **Other cookies than "strictly necessary" cannot be installed to a browser/device before a user has given a consent**.
  - For example, analytical cookies, social media and marketing cookies need a prior consent.

EXAMPLES FROM OTHER CASES

- A provider of hospital booking system collected and further processed personal data (including health data) without a valid legal basis.
  - DPA found out that the provider, particularly in the context of health data resulting from appointment bookings at health care facilities, had no legal basis for the processing and violated the principle of storage limitation.
  - Administrative fine of EUR 40.000 (Italy).
- Unnecessarily long retention period and incomplete anonymization of personal data
  - Administrative fine of EUR 160,000 (Denmark).
- Absence of a data processing agreement
  - Administrative fine of EUR 5000 (Germany).
- Incomplete information on camera surveillance and too large area covered by a camera surveillance
  - Administrative fine of EUR 4800 (Austria).

DATA TRANSFERS OUTSIDE THE EU/EEA

LEXIA
Legal Excellence

TRANSFER OF PERSONAL DATA OUTSIDE THE EU/EEA

AN ADEQUACY DECISION

European Commission decision on adequacy of data protection (Argentina, Canada, Israel, Japan, New Zealand, Switzerland, Uruguay)

~~Privacy Shield mechanism~~

APPROPRIATE SAFEGUARDS

Standard contractual clauses (SCCs)
Binding corporate rules (BCR)
Approved code of conduct / sertificates

DEROGATIONS

Explicit consent
Contractual (or pre-contractual necessity)
Necessity to protect vital interests
Necessity due to legal claims

Personal data transfer to the United States

- In July 2020, the Court of Justice of the European Union (CJEU) issued a ruling on data protection and transfer of personal data to the US (“Schrems II”).
- According to the CJEU ruling, the Privacy Shield mechanism does not meet the requirements set out in the Data Protection Regulation.
- Transfer of personal data under the Privacy Shield system **is not permitted** as of July 16, 2020.
- Transfer of personal data based on e.g. standard contractual clauses is still permitted (with necessary supplementary measures)

WHAT SHOULD BE DONE NOW?

1. **Review** your service providers and other processors to determine which of these transfer or otherwise process personal data outside the EU/EEA
   - providing access to personal data outside the EU/EEA or passive retention outside the EU/EEA means under the GDPR a transfer of personal data to third countries
2. **Replace** the Privacy Shield mechanism with other transfer mechanisms, such as standard contractual clauses (with supplementary safety measures if necessary).
   - Needs to be done in co-operation with a recipient of personal data
3. **Follow** the authorities' guidance on the matter also regarding **supplementary measures**
   - Recommendations 02/2020 on the European Essential Guarantees for surveillance measures.
   - Recommendations 01/2020 on the measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data
4. **Update** privacy policies, DPAs and other privacy information
   - Data subjects shall be informed of the transfer of personal data outside the EU/EEA and applicable transfer mechanism
   - Update DPAs (Data Processing Agreements) / amend SCCs
5. Note that if there is no supplementary measure available to ensure an appropriate level of data protection, processing must be suspended or ceased.
   - Alternatively, a competent DPA must be notified, and data subjects be informed.

TRANSFER OF PERSONAL DATA OUTSIDE THE EU/EEA

LEXIA ATTORNEYS LTD

MARKUS MYHRBERG

+358 40 5055343
markus.myhrberg@lexia.fi

VILLE KUKKONEN

+358 40 7456784
ville.kukkonen@lexia.fi