

ROJS PELJHAN PRELESNIK
& PARTNERS

Special categories of personal data



Law firm

Sandra Kajtazović, attorney-at-law
CIPP/E, CIPM

Roadmap

I. Scope and definitions

II. Case study

- 3 recent enforcement cases and main points of focus

III. Secondary use of data for research purposes

I. The Basics - Scope and definitions

- In general, GDPR covers all processing of personal data
- Does not apply to anonymous information
- Definition of special categories of personal data (“sensitive” data)
 - Race and ethnic origin
 - Religious or philosophical beliefs
 - Political opinions
 - Trade union memberships
 - Biometric data used to identify an individual
 - Genetic data
 - Health data
 - Data related to sexual preferences, sex life, and/or sexual orientation
- Processing of sensitive data generally prohibited unless one of 10 conditions from Article 9(2) GDPR applies.
- **Wide open doors:** MS may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.

Lawful basis for processing special category data

- identify a lawful basis under Art. 6 + a separate condition under Art. 9(2) GDPR.

Conditions for processing special category data:

a) explicit consent

b) 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** (EU or MS law or collective agreement)

c) necessary to protect the vital interests of the data subject or of another natural person

d) processing by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim of their (former) members data

e) personal data which are manifestly made public by the data subject

f) necessary for the establishment, exercise or defence of legal claims

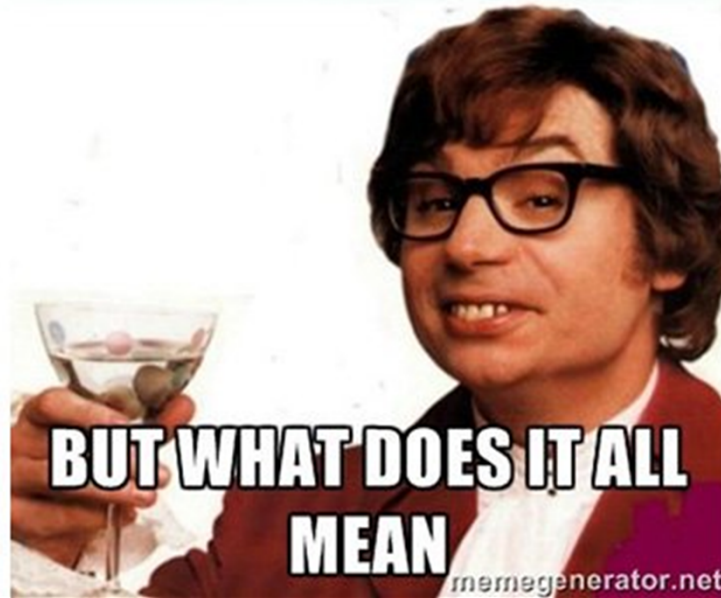
g) necessary for reasons of substantial public interest, on the basis of EU or MS law

h) necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of EU or MS law or pursuant to contract with a health professional

i) necessary for reasons of public interest in the area of public health (EU or MS law)

j) necessary for archiving purposes in the public interest, **scientific or historical research purposes** or statistical purposes in accordance with Article 89(1) based on EU or MS law

WOOPY DOO BASIL



**BUT WHAT DOES IT ALL
MEAN**

memegenerator.net

II. Case study

Case 1: Facial recognition in Swedish school (22. 8. 2019)

Case 2: Austrian controller in the medical sector (12. 8. 2019)

Case 3: Austrian Post and data on political opinions (23. 10. 2019)

Source: <https://edpb.europa.eu/>

Case 1: Facial recognition in Swedish school (22. 8. 2019)

Facts: A school in northern Sweden conducted a pilot project using facial recognition technology to keep track of students' attendance in school. Attendance of 22 students over a period of 3 weeks was taken with the help of facial recognition technology, instead of a regular "call". The school has based this processing on students' consent.

What did the DPA say:

- Insufficient legal basis for data processing (Art. 9 GDPR, Art. 5(1) c) GDPR)
- Failure to do an adequate DPIA (35 GDPR)
- Failure to consult DPA (Art. 36 GDPR)

Imposed fine: 200 000 SEK (approx. 20.000 EUR)

Case 1: Points of attention

1. Consent (Art. 4(11) & Art. 7 GDPR)

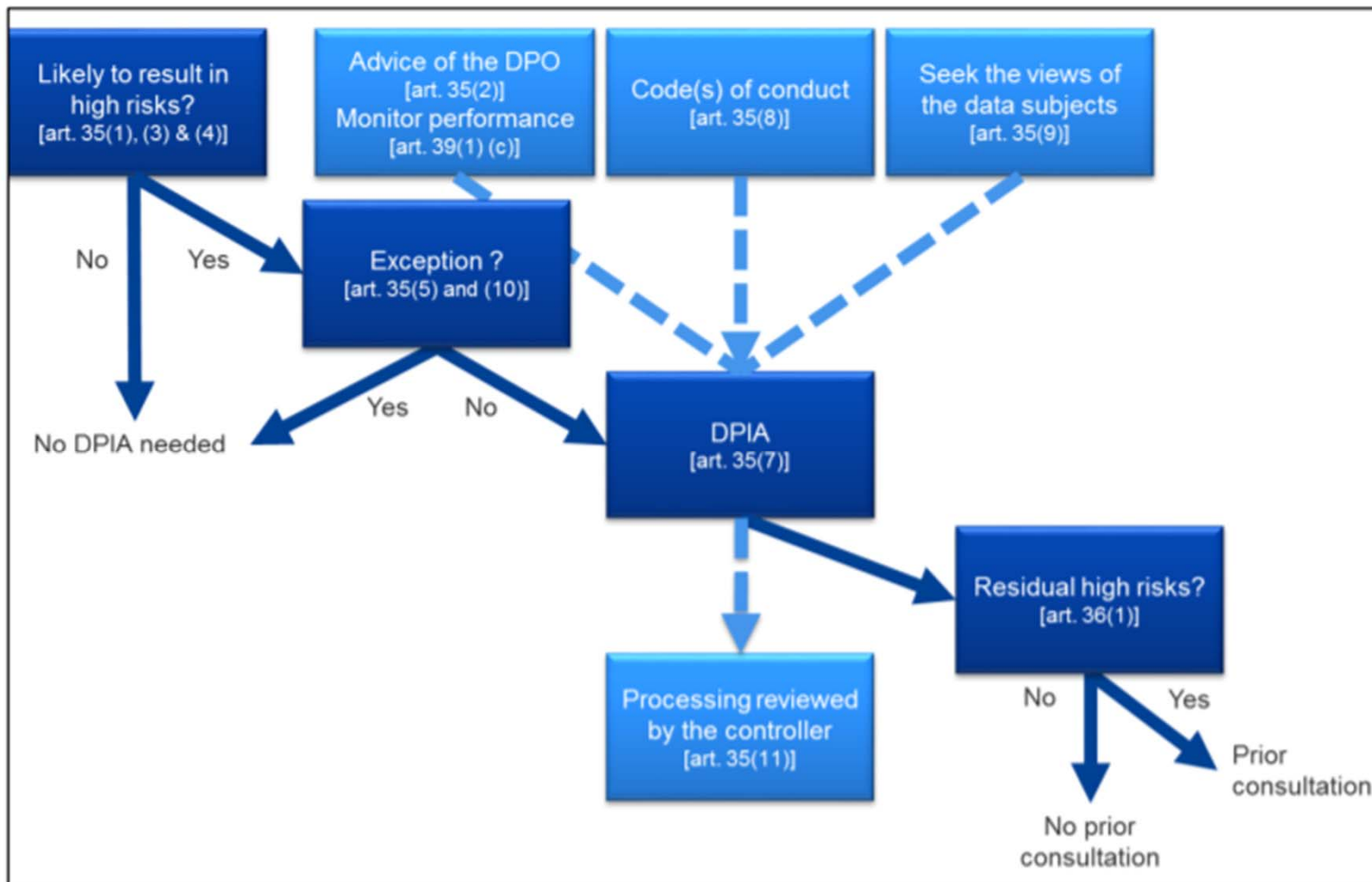
- Conditions for consent

To be valid, consent to processing of personal data must:

- be *freely given, specific and unambiguous*
 - be explicit for special category data – not defined in the GDPR
 - be a *clear affirmative action*
 - cover *all processing activities* carried out for the same purpose → address foreseeable use, including secondary use
- Consent is not *freely given*, where there is a *clear imbalance* between the data subject and the data controller (Rec. 43 GDPR) (e.g. employee/employer; in clinical studies: patients, who are not in good health conditions, when they belong to an economically or socially disadvantaged group, in any situation of institutional hierarchical dependency).
 - Consent is presumed not be *freely given*, if:
 - the data subject was unable to withdraw or refuse consent without detriment
 - the data subject has no genuine and free choice
 - it does not allow separate consent to be given to different data processing operations

2. DPIA (Art. 35 GDPR) + consultation with DPA (Art. 36 GDPR)

- DPIA is an assessment to identify and minimise non-compliance risks.



Source: WP 248 rev.01, p.7.

- **Controllers must ensure that a DPIA has been run on any “*high risk*” processing activity before it is commenced.**
 - “*large scale*” processing of sensitive data, profiling activities which produce legal effects/significantly affect individual, or systematic monitoring of a public area on a “*large scale*” are cited as (non-exhaustive) examples of high-risk processing.
 - in assessing “*large scale*” processing WP29 recommends considering the number of data subjects concerned (no. or % of relevant population), volume of data, duration of processing, geographical extent of processing activity.
- **Processing operations which may require a DPIA include** AML/CTF screening, biotechnology company offering genetic tests directly to customers to assess/predict disease/health risks, building behavioural or marketing profiles based on usage or navigation on website, processing that might lead to exclusion or discrimination of individual, private investigator keeping offenders’ details, processing including vulnerable data subjects (e.g. children, employees, mentally ill persons, elderly, patients, etc.), innovative use of new technology, IoT.
- **As a minimum, the GDPR requires that a DPIA include:**
 - A description of the processing activities and their purpose
 - An assessment of the necessity and proportionality of processing operations and risks to data subjects
 - Measures to address the risks

Case 2: Austrian controller in the medical sector (12. 8. 2019)

Facts: Controller based certain processing of patients' personal data on consent. The consent form obliged data subjects to give their consent to the transfer of their personal data to third parties (possibility of separate consent was not offered) and stated that consent was irrevocable. Controller provided information as the legal basis for data processing under Article 6 GDPR, but failed to provide information regarding the special condition under Article 9(2) GDPR for processing of special category data. Further, controller did not appoint a DPO and did not carry out a DPIA.

What did the DPA say:

- Insufficient fulfilment of information obligations (Art. 13 GDPR)
- Insufficient legal basis for processing (Art. 7 GDPR)
- Failure to do a DPIA (Art. 35 GDPR)
- Breach of duty to appoint a DPO (Art. 37 GDPR)

Imposed fine: 50.000 EUR

Case 2: Points of attention

1. DPO appointment (Art. 37 GDPR)

- *MS law* – You are required to do so by national law;
 - *Public authority* – You are a public authority or body (other than a court);
 - *Regular and systematic monitoring* – Your core activities consist of *regular and systematic monitoring* of data subject on a *large scale*; or
 - *Special category data* – Your core activities consist of processing special category personal data on a *large scale* (including processing information about criminal offences).
- DPO must be involved in all data protection issues.
 - DPO cannot be dismissed or penalised for performing their role.
 - DPO must report directly to the highest level of management.
 - Group companies can appoint a single DPO.
 - DPO can be a member of staff or a hired contractor.

Case 3: Austrian Post and data on political opinions (23. 10. 2019)

Facts: Austrian Postal Service had created profiles of more than 3 million Austrians, which included information about their home addresses, personal preferences, habits and possible political party affinity by using statistical calculation methods – these profiles were then sold to third parties. In addition, it was found that the company carries out “*further processing of data on package frequency and the frequency of relocations for the purpose of direct marketing*” without legal basis. The Austrian Post argued that it did not collect *sensitive personal data*, but rather processed statistical information.

What did the DPA say:

- Austrian Post processes special category data on alleged political affinity.
- No legal basis for processing alleged political affinity (Art. 9 GDPR, 5(1)a) GDPR)
 - data subjects did not give explicit consent

Imposed fine: 18 million EUR (not yet final)

Case 3: Points of attention

1. Definition of special category data

- data that can be used in itself or in combination with other data to draw a conclusion about e.g. individual's health, beliefs can be considered sensitive data

WP - Advice paper on special categories of data (“sensitive data”), April 2011

The term “data *revealing* racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership” is to be understood that not only data which by its nature contains sensitive information is covered by this provision, but also data from which sensitive information with regard to an individual can be concluded.

- DPAs already take expansive view of health data
- Performance data becomes health data
- GDPR, Rec. 35: “information derived from the testing or examination of a body part or bodily substance, including from genetic and biological samples” is sensitive data

Dutch DPA finds fitness app violates data protection law

The Dutch Data Protection Authority (College bescherming persoonsgegevens, hereinafter ‘CBP’) published a report on 11 November following an investigation into Nike’s fitness app, the Nike+ Running app. The CBP found several violations of data protection law, according to its nearly hundred-page report. The report is interesting in that it provides detailed insight into how the Dutch Data Protection Authority views personal data concerning health and the thought processes behind the concept of health data, as Sofie van der Meulen and Erik Vollebregt of Axon Lawyers explain.

● Nike has no legal basis to process and use other information that is obtained from the smartphone, such as location information and contact information. Although Nike does inform users in more general terms about the processing and use of their data and asks for permission for the use of data, this information is not sufficient to establish informed consent. Based on the provided information, users are not able to determine the scope of the use of their data and cannot establish exactly what they give permission for. Therefore, there is no legally valid consent as a basis for the processing of personal data.

Does Nike process health data?

The Nike+ Running app is the first

time is created of all registered and calculated data for a specific user. Thus Nike has access to the sporting performance of a user over time. With this insight, Nike can conclude whether the physical condition of a user improves or deteriorates. According to the CBP, such information on a person’s physical condition qualifies as health data as it provides information about the health of the user. The indefinite retention of the obtained data forms another factor to qualify the obtained data as health data because it allows a profile to be built up over time.

The deduced effect of practising sports on a person’s condition: health data

Nike discussed with the

III. Secondary use of data for scientific research purposes

- **Three alternative legal bases:**

1. **Legitimate interests under Article 6(1)(f) in conjunction with Article 9(2) (j) GDPR**

- EU or MS law may allow processing for research purposes with *appropriate safeguards* (Art. 89(1) GDPR).
 - o Be aware: national legislation may also prohibit certain secondary uses!
 - o Technical and organizational measures to ensure data minimizations. Those may include pseudonymization.

2. Under specific circumstances, when all conditions are met, **data subject's explicit consent under Article 6(1)(a) and 9(2)(a) GDPR**

- "Broad consent" is normally not allowed, but it may be possible to obtain consent for *areas or parts of research projects* (Rec. 33 GDPR).

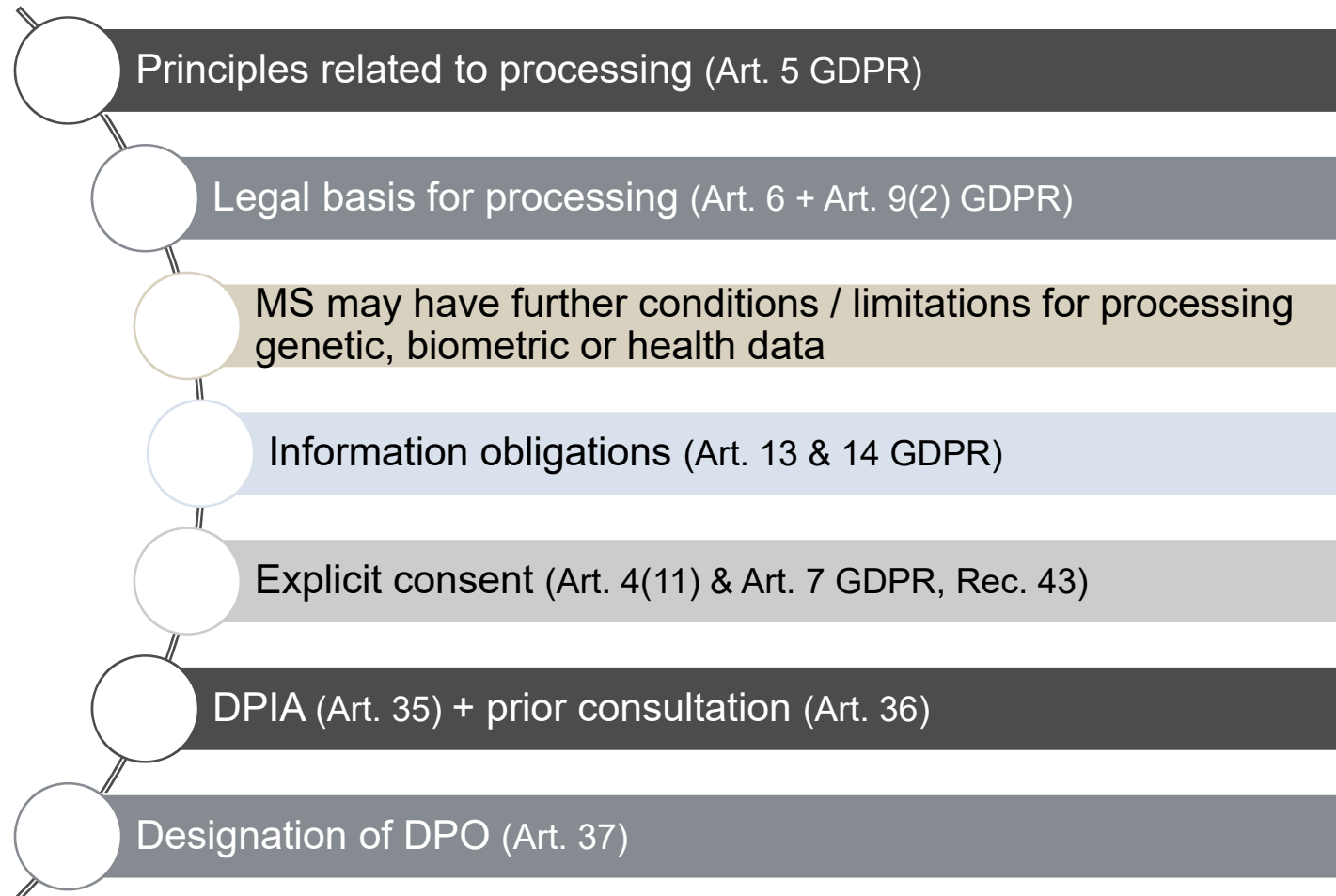
3. **Art. 5(1)(b) GDPR:** Where data is further processed for scientific research purposes, these shall *a priori not be considered as incompatible* with the initial purpose, provided that specific adequate safeguards and derogations are in place (Art. 89 GDPR).

- Under certain conditions controller could be able to further process the data without the need for a new legal basis (Rec. 50 GDPR).
- These conditions will require specific attention and guidance from the EDPB in the future.
- See EDPB Opinion 3/2019 o interplay between CTR and GDPR.

- **EU or Member State law may derogate from certain rights of data subjects** *in so as such rights are likely to render impossible or seriously impair the achievement of the specific purposes* (Art. 89(2) GDPR)

Processing special category data?

Main points to consider



ROJS PELJHAN PRELESNIK
& PARTNERS

Thank you

Sandra Kajtazović, attorney-at-law

CIPP/E, CIPM

Phone: +386 1 23 06 750

E-mail: kajtazovic@rppp.si



Law firm