KILPATRICK TOWNSEND

Overview of the EU General Data Protection Regulation

Jon Neiditz
jneiditz@kilpatricktownsend.com
https://www.linkedin.com/in/informationmanagementlaw
(404) 815-6004

NCVHS

KILPATRICK TOWNSEND

Whether the GDPR Applies Later This Month

European Data Protection Directive 95/46 applies to	General Data Protection Regulation 2016/679 applies to
A data controller where it is established in an EU Member State and the data is processed in the context of that establishment	The processing of personal data in the context of the activities of a data controller or data processor established in the EU, irrespective of where the processing takes place
A data controller where it is not established in an EU Member State, but is **using equipment in an EU Member State** for processing data otherwise than for the purposes of transit through that Member State	The processing of personal data of data subjects who are in the EU by a data controller or data processor not established in the EU, where the processing activities are related to: • The **offering of goods or services to those data subjects**; or • The **monitoring of their behavior in the EU**

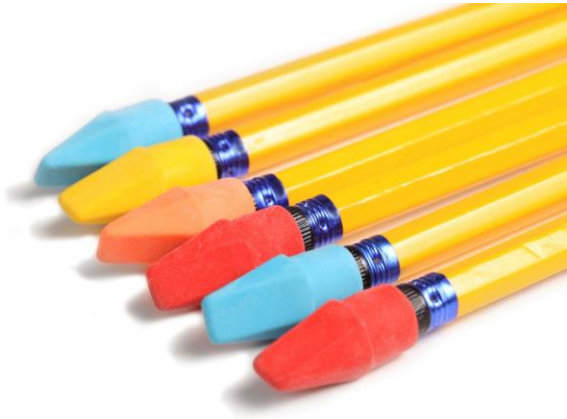
KILPATRICK TOWNSEND

Key EU GDPR Principles

- Under Article 5 of the GDPR, Personal Data must be:
  - processed lawfully, fairly and in a transparent manner
  - collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
  - adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimization')
  - accurate and, where necessary, kept up to date ('accuracy');
  - 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 ('storage limitation')
  - processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ('integrity and confidentiality').

KILPATRICK TOWNSEND

Key EU GDPR Terminology



Personal Data

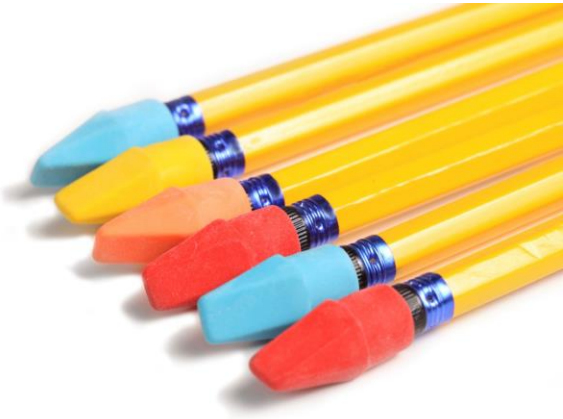
Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Processing

Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

KILPATRICK TOWNSEND

Key EU GDPR Terminology (cont'd)

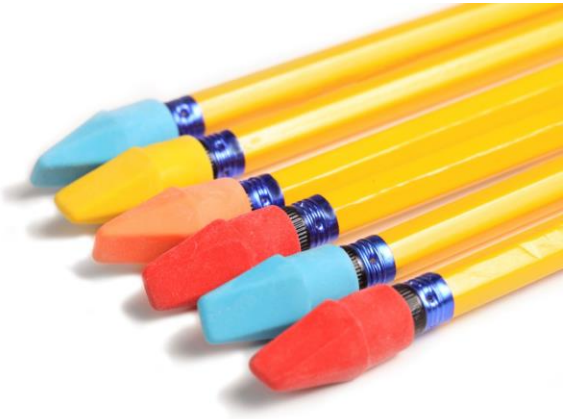


Special Categories of Personal Data

Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

KILPATRICK TOWNSEND

Key EU GDPR Terminology (cont'd)



Data Controller

The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Data Processor

A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

KILPATRICK TOWNSEND

Data Controller vs. Data Processor - Who is Who?

The Data Controller decides:

- whether to collect the personal data and the legal basis for doing so;
- which items of personal data to collect;
- the purpose the data are to be used for;
- which individuals to collect data about;
- whether to disclose the data, and if so, to whom;
- whether subject access and other individuals' rights apply; and
- how long to retain the data.

The Data Processor may decide:

- what IT systems or other methods to use to collect, store and transfer personal data;
- the detail of the security surrounding the personal data;
- the means used to retrieve personal data about certain individuals;
- the method for ensuring a retention schedule is adhered to; and
- the means used to delete or dispose of the data.

KILPATRICK TOWNSEND

Key Elements of the GDPR

- **Extraterritorial Reach -** applies to any processing of personal data related to EU citizens and non-EU citizens located in the EU, even where the data controller is located in a country outside of the EU, if processing relates to the offering of goods/services to such individuals or monitoring their behavior.
- **Fines** – companies could be fined up to the greater of 4% of global turnover or 20 million Euros.
- **Data Protection Officers (DPOs)** – DPOs required if core activities consist of processing operations, which require regular and systematic monitoring of data subjects on a large scale or process on a large scale special categories of data.
- **Security Breach Notifications** – controllers must notify DPAs within 72 hours of the breach.
- **The Right to Be Forgotten** – individual's right to demand deletion of online content.
- **Data Portability** - individuals must be able to transfer personal data from one service provider to another more easily.

KILPATRICK TOWNSEND

Key Elements of the GDPR (continued)

- **Consent** - stricter rules on obtaining consent, with companies no longer able to rely on "opt-outs“ or pre-checked boxes to justify data processing. Consent must be either (i) unambiguous consent for general processing of personal data; or (ii) explicit consent for processing of special categories of personal data.
- **Processors** - direct obligations placed on data processors for the first time, including specific new requirements for existing and new data processing contracts.

KILPATRICK TOWNSEND

Key Elements of the GDPR (continued)

- **One Stop Shop** - Pan-European business will have a lead data protection regulator in the EU country where it is mainly established.
- **Profiling** - automated decision-making (including profiling) that either produces a **legal effect or significantly affects** individuals must be (i) authorized by law; or (ii) necessary to enter into or perform a contract with that individual; or (iii) based on individual's explicit consent.
- **Minors** - consent must be obtained from parents or legal guardians when information society services are provided to minors below the **age of 16**.

KILPATRICK TOWNSEND

Key Elements of the GDPR (continued)

- **Accountability** - GDPR introduces new explicit principle of accountability – data controllers must ensure compliance with the general data processing principles.
- **Records of processing activities** - No more DPA registrations, **but** controllers and processors must maintain internal records of all the data processing activities under their responsibility.

KILPATRICK TOWNSEND

Key Elements of the GDPR (continued)

- **Privacy by Design / Privacy by Default** - GDPR introduces new concepts of "**privacy by design"** and "**privacy by default"**. The controller must implement **appropriate technical and organizational measures,** which are designed to integrate the necessary safeguards into the processing.
- **Data Protection Impact Assessments** - data controller must carry out a **data protection impact assessment** prior to processing data, where the processing is likely to result in a high risk to the rights / freedoms of individuals due to (i) the use of new technologies; or (ii) the nature, scope, context, and purposes of processing.

KILPATRICK TOWNSEND

GDPR Protects Rights…

https://www.eugdpr.org/eugdpr.org.html

KILPATRICK TOWNSEND

A Record of All Personal Data Processing

- The GDPR requires a detailed record of data processing activities, a “register,” which is the main document to be shared with regulators.
- You need to understand your data in order to comply with various GDPR obligations. Data mapping can be done in order to determine the types of data you are collecting, the purposes for which it is being processed, how it was obtained, and the parties that it is being shared with.
- Types of data: understand types of data recognized by GDPR (new elements of personal data, sensitive personal data, pseudonymous data...).
- Purposes for processing: assess “grounds for processing” to ensure that it is appropriately limited
- How it was collected: need to know how data was obtained in order to evaluate new consent rules.
- Parties involved: GDPR includes new obligations with regard to third party contracts, but you also must know which party bears responsibility for compliance.

KILPATRICK TOWNSEND

Data Protection Impact Assessments (DPIAs)

- A DPIA is an assessment to identify and minimize non-compliance risks.
- Specifically, controllers must ensure that a PIA has been run on any *"high-risk"* processing activity before it is commenced – focused on the risk of infringing a natural person's rights and freedoms.
- *"Large scale"* processing of sensitive data, or profiling activities, are cited as illustrative examples of high-risk processing. DPAs will publish details of further examples and guidance.
- As a minimum, the GDPR requires that a DPIA include:
  - A description of the processing activities and their purpose;
  - An assessment of the need for, and proportionality of, the processing, and the risks arising and measures adopted to mitigate those risks, in particular safeguards and security measures to protect personal data and comply with the GDPR.

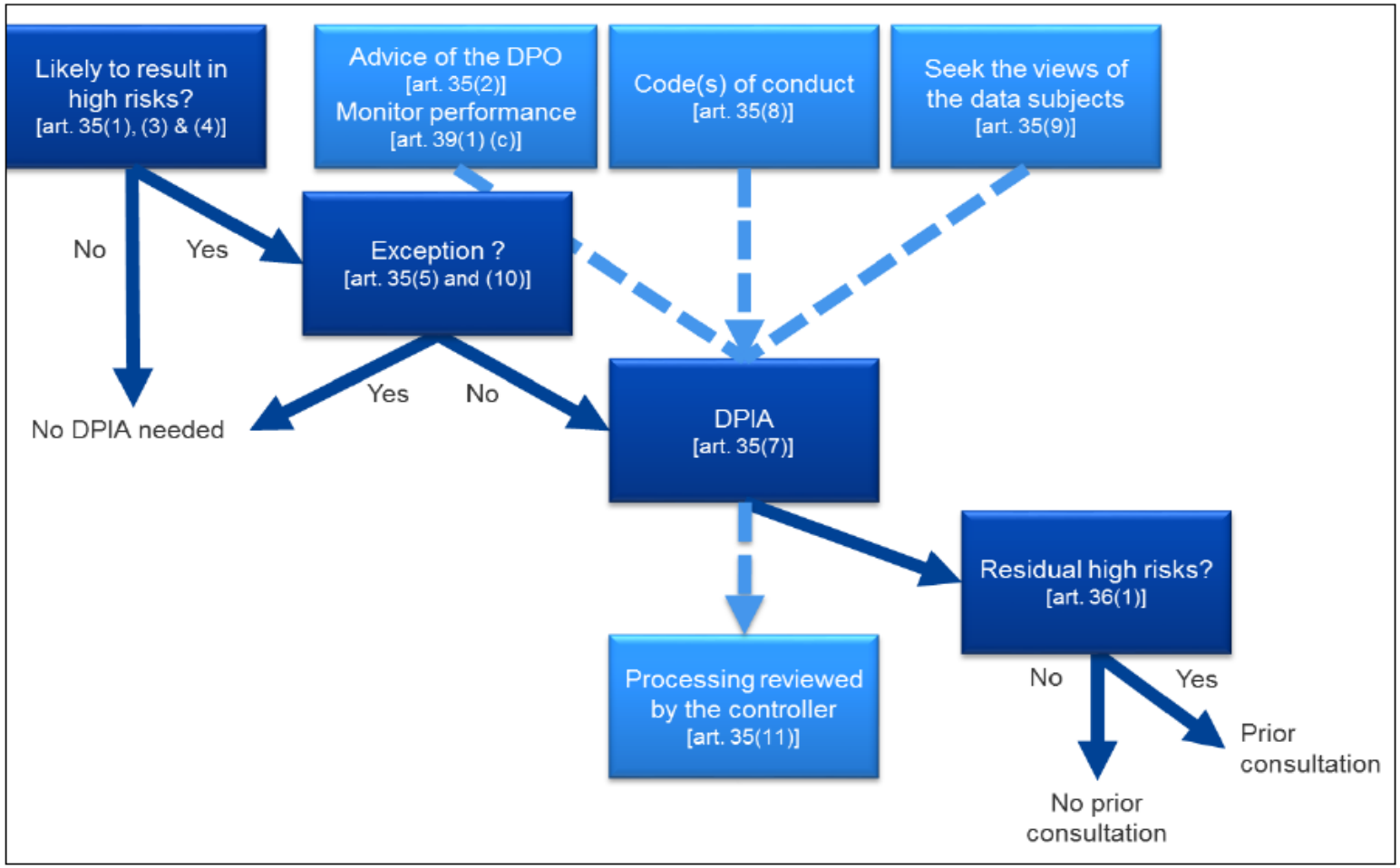
KILPATRICK TOWNSEND

"High-Risk" (WP 248)

- "Evaluation or scoring (including profiling and predicting)."
- "Automated decision making with legal or similar significant effect."
- "Systematic monitoring."
- "Sensitive data or data of a highly personal nature."
- "Data processed on a large scale."
- "Matching or combining data sets."
- "Data concerning vulnerable data subjects."
- "Innovative use or applying new technological or organizational solutions."
- "[W]hen the processing (prevents data subjects from exercising a right or using a service or a contract."

KILPATRICK TOWNSEND

DPIA Process (WP 248)



KILPATRICK TOWNSEND

ANCHORAGE
ATLANTA
AUGUSTA
CHARLOTTE
DALLAS
DENVER
HOUSTON
LOS ANGELES
NEW YORK
RALEIGH
SAN DIEGO
SAN FRANCISCO
SEATTLE
SHANGHAI
SILICON VALLEY
STOCKHOLM
TOKYO
WALNUT CREEK
WASHINGTON D.C.
WINSTON-SALEM