Welcome!

In today’s information economy, the risks—and opportunities—associated with the use and collection of data continue to skyrocket. But you probably already know that.

You probably also know that skilled privacy pros are in high demand. After all, that is one of the reasons you are here, right?

You have come to the right place. The IAPP is the world’s largest information privacy organization. We are a non-advocacy, not-for-profit membership association focused on advancing the privacy profession.

Our globally recognized privacy training is designed to give you the expertise and know-how you need to get ahead. You will hear from world-class privacy faculty who are experts working in the field of privacy and data protection today. They will share their knowledge, insights and real-life experiences to help you sharpen your skills and work smarter—not to mention, take your career to a whole new level.

Whether you are a seasoned professional or new to the field of privacy and data protection, this class is an opportunity to learn essential skills, and, if you decide to aim for an IAPP credential, you will have a head start!

Thank you for joining us today.
Acknowledgements

Thank you to the following IAPP instructors, members and subject matter experts who provided their guidance and expertise to the development of this training:

Jeroen Terstegge  
CIPP/E, CIPP/US  
Partner  
Privacy Management Partners

Phil Lee  
CIPP/E, CIPM, FIP  
Partner  
Privacy, Security and Information  
Fieldfisher

Mark Webber  
CIPP/E  
U.S. Managing Partner  
Fieldfisher (Silicon Valley) LLP

Olivier Proust  
CIPP/E  
Partner  
Privacy, Security and Information  
Fieldfisher

Bavo Van den Heuvel  
CIPP/E, CIPP/US, CIPM, CIPT, FIP  
Chief Knowledge Officer - Partner, Strategic  
Advisor  
Cranium Applied Privacy

Michaela Buck  
External DPO

Orrie Dinstein  
CIPP/US  
Global Chief Privacy Officer  
Marsh & McLennan Companies

Bob Siegel  
CIPP/C, CIPP/E, CIPP/G  
CIPP/US, CIPM, CIPT, FIP  
President  
Privacy Ref, Inc
Acknowledgements

Thank you to the following IAPP instructors, members and subject matter experts who provided their guidance and expertise to the development of this training:

Sachin Kothari  
CIPP/US  
Managing Director, Consumer Digital Privacy and Compliance  
AT&T

Nick Graham  
CIPP/E  
Partner  
Dentons

Judy Macior  
CIPP/C, CIPP/G, CIPP/US, CIPT, FIP  
VP Compliance & Information Practices  
Experian

Aurélie Pols  
DPO CDP mParticle  
Data Governance & Privacy Engineer  
EDPS’s EAG member  
Competing on Privacy S.L.

Gabe Maldoff  
CIPP/US  
Privacy and Data Protection Associate  
Covington & Burling LLP

Anna Myers  
CIPP/US, CIPM  
Attorney Fellow  
ZwillGen PLLC
Trainer introduction
European Data Protection

Chat: Share

How would you describe your industry?
How many years have you worked in privacy?

Chat: Share
How many years have you worked in privacy?
Course outline

- Module 1: Data protection laws
- Module 2: Personal data
- Module 3: Controllers and processors
- Module 4: Processing personal data
- Module 5: Data subject rights
- Module 6: Information provision obligations
- Module 7: International data transfers
- Module 8: Compliance considerations
- Module 9: Security of processing
- Module 10: Accountability
- Module 11: Supervision and enforcement

Course outcomes

This course will ...
- Define key concepts of European data protection
- Describe EU data protection laws and regulatory bodies
- Explain the application of the GDPR and other compliance obligations to European and international entities

Note

While examples from member state data protection laws may be referenced by your trainer, this training will focus on the broader EU Regulation.
Module 1: Data protection laws

Learning objectives

- Differentiate between the Council of Europe and the European Union, including member state composition and legislation related to privacy and data protection
- Describe the history of human rights, privacy, and data protection law in Europe leading up to the current EU legislative framework
- Recognise themes in human rights and data protection law, including right to privacy and freedom of speech, and the balance between the two
- Describe the functions of the EU’s legislative, policy-making and judicial institutions, specifically as they apply to data protection law
- Describe the EU data protection law’s transition from a directive that requires member state transposition to a regulation
Which type of privacy is most important to your *personal* life? Information privacy, territorial privacy, bodily privacy, or communication privacy?

- Information privacy
- Territorial privacy
- Bodily privacy
- Communication privacy
Chat: Share

Which type of privacy is most important to your *professional* life? Information privacy, territorial privacy, bodily privacy, or communication privacy?

- Information privacy
- Territorial privacy
- Bodily privacy
- Communication privacy
Session notes

The European Union and the Council of Europe
- Separate European institutions
- Own laws and judicial systems
- Council of Europe membership much larger than EU
- All EU member states belong to Council of Europe, but not vice versa

European Union
- 27 member states
  - On 31 January 2020, the U.K. exited the European Union
- Economic and political union
- Privacy and data protection laws
  - Charter of Fundamental Rights of the EU (CFREU)
  - Treaty on the Functioning of the EU (TFEU)
  - General Data Protection Regulation (GDPR)
  - ePrivacy Directive
  - National data protection laws across Europe

Council of Europe
- 47 member states
- International organisation
- Privacy and data protection laws
  - European Convention on Human Rights (ECHR)
  - CoE Convention (also called Convention 108)
Session notes

EU member states: Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain and Sweden

The European Economic Area (EEA) is an economic region that includes the European Union (EU) and Iceland, Norway and Liechtenstein—which are not official members of the EU but are closely linked by economic relationship. Non-EU countries in the EEA are required to adopt EU legislation regarding the single market.

- Based on the Agreement of the European Economic Area (1994)
- Allows members of the European Free Trade Association (EFTA) to participate fully in the internal market

Switzerland is not part of the EEA Agreement but does have a bilateral agreement with the EU.

European Free Trade Association (EFTA): Iceland, Liechtenstein, Norway and Switzerland

United Kingdom: The U.K. formally left the European Union on 31 January 2020. The Trade and Cooperation Agreement signed between the EU and U.K. on 24 December 2020 allows the transfer of personal data from the EU to the U.K. to continue for up to six-months while the European Commission proceeds with adequacy assessments under the EU GDPR and the Law Enforcement Directive.
Privacy and data protection laws

<table>
<thead>
<tr>
<th>Charter of Fundamental Rights of the EU</th>
<th>European Convention on Human Rights</th>
</tr>
</thead>
<tbody>
<tr>
<td>European Union</td>
<td>Council of Europe</td>
</tr>
<tr>
<td>Lisbon Treaty (TFEU)</td>
<td>Member state ratification</td>
</tr>
<tr>
<td>Article 7: Private life, family life, home, communications</td>
<td>Article 8: Protects private life, family life, home, communications</td>
</tr>
<tr>
<td>Article 8: Establishes a separate right to data protection</td>
<td>Article 8: Includes the right to data protection <em>(private life)</em></td>
</tr>
</tbody>
</table>

**Module 1: Data protection laws**

**Session notes**

**Charter of Fundamental Rights of the EU (CFREU), 2000**
- Comprehensive collection of individual rights
- Enshrined fundamental rights which became binding through the Treaty of Lisbon (2007)
- Limitations provided for by law
- Respect the essence of the right
- Genuinely meet the objectives of general interest recognised by the EU or the need to protect the rights and freedom of others
- Necessary and proportionate

Interpretation of the CFREU may not contravene the ECHR, but may provide for higher level of protection.

**European Convention on Human Rights (ECHR), 1950 (entered into force 1953)**
- Member state ratification
  - Based on the Universal Declaration of Human Rights
  - Key document for fundamental rights in Europe (not only the EU)
- In accordance with the law
- Necessary in a democratic society
  - Public security and safety
  - Economic well-being of country
  - Prevention of disorder or crime
  - Protection of health or morals
  - Protection of rights and freedoms of others
- Article 8 is considered to be one of the Convention’s most open-ended provisions
Comparing European courts

<table>
<thead>
<tr>
<th>Court of Justice of the EU</th>
<th>European Court of Human Rights</th>
</tr>
</thead>
<tbody>
<tr>
<td>Judicial body of the European Union</td>
<td>Part of the apparatus of the Council of Europe</td>
</tr>
<tr>
<td>Decides on issues of EU law and enforces those decisions</td>
<td>Enforces European Convention on Human Rights and Convention 108</td>
</tr>
<tr>
<td>Comprises of the Court of Justice (ECJ) and the General Court (renamed ‘Court of First Instance’, CFI)</td>
<td>Judges sit in their individual capacity and do not represent any state</td>
</tr>
<tr>
<td>Data protection as it relates to cases brought by national courts and by the Commission against member states</td>
<td>Data protection as it relates to Article 8</td>
</tr>
</tbody>
</table>

Session notes

Based in Luxembourg, the Court of Justice of the EU is the judicial body of the EU. It makes decisions on issues of EU law and enforces decisions, either in respect of actions taken by the European Commission against a member state or by an individual or organisation to enforce their rights under EU law. The Court comprises the European Court of Justice (ECJ) and the General Court. The Court provides clarification of EU law to national courts to assist the national courts in upholding EU law. Relevant landmark cases include:

- Bodil Lindqvist v Åklagarkammaren i Jönköping, Nowak v Data Protection Commissioner
- Google Spain v AEPD and Mario Costeja González, Schrems v Data Protection Commissioner, Data Protection Commission v. Facebook Ireland, Schrems
- Weltimmo s. r. o. v Nemzeti Adatvédelmi és Információszabadság Hatóság Judgment

The European Court of Human Rights (ECHR) in Strasbourg upholds privacy and data protection laws through its enforcement of the European Convention on Human Rights and Convention 108. It is not part of the European Union. The ECHR has also considered the question of the protection of personal data from the viewpoint of the right of access to such data. Relevant landmark cases include:

- Niemietz v Federal Republic of Germany, Halford v United Kingdom, Copland v United Kingdom
- Bărbulescu v Romania
- I v Finland
Session notes

Data protection: Dawn of a new age

- 1960s
  - Economic and technological advancements
    - Increasing international trade
    - Use of computers and telecommunications

- 1970s
  - Conflict between national privacy rights and international free trade
  - Development of communication technologies
    - Extensive banks of personal data
    - New opportunities for international data processing

- Developing concerns
- Government collection and use of data
- Collection of consumer data

Module 1: Data protection laws
Session notes

The privacy tug of war: right to privacy vs. freedom of speech

• Contradiction between two fundamental human rights
• Increasing relevance in the information age
• Right to withdraw consent
• Right to lodge a complaint
Case study

Google Spain v. AEPD and Mario Costeja González

Mr. Costeja sued Google Spain, Google Inc. and La Vanguardia newspaper because personal data about him was available through a Google search in the newspaper’s online archives. The Court of Justice of the EU ruled that Google Spain must remove the links to the article.

Note: The issue around a platform’s responsibility related to content curation—what is accepted and what is not in light of globalisation—predates the Costeja case (e.g., LICRA v. Yahoo!).

Data protection laws
The privacy tug of war

Module 1: Data protection laws
Session notes
An evolving harmonised approach

  - Nonbinding
  - Protection of personal data in a global economy
  - Principles on collection and use
  - 2013 revision
Data protection laws
An evolving harmonised approach

1980
OECD Guidelines

1981
Convention 108

Session notes
An evolving harmonised approach

  • Legally binding treaty of member states (also open to nonmembers) of the Council of Europe
  • Protection of data subject privacy
  • Automatically processed personal data

*In October 2018, Convention 108+, a version of Convention 108 overhauled to align with the GDPR, was signed by 20 states of the Council of Europe, including the UK. Since then, more states have followed. According to the European Commission, it serves as a means for third countries (those outside the EU) to adopt the basic tenets of the GDPR.
Data protection laws
An evolving harmonised approach

OECD Guidelines Convention 108 The EU Data Protection Directive

Module 1: Data protection laws

Session notes
An evolving harmonised approach
• 1995: The EU Data Protection Directive (95/46/EC)
  • Legally binding transposition of member states of the EU
Session notes
An evolving harmonised approach
• 2000:
  • Charter of Fundamental Rights of the EU
  • The E-Commerce Directive of 2000 (Directive 2000/31/EC)
    • Issues related to processing personal data excluded from its scope
Session notes
An evolving harmonised approach

- **2002:** The EU Directive on Privacy and Electronic Communications (ePrivacy Directive/Cookie Directive)
  - Communications passed over electronic channels
  - Particular rules around marketing, cookies, and security breach notifications for internet service providers (ISPs) and telecommunications companies
  - 2009 amendment
Session notes

An evolving harmonised approach

  - Requirements of ISP and telecommunication companies to keep metadata about the communications they carried in case it needed to be accessed for law enforcement purposes
  - 2014 Digital Rights Ireland case—validity of the Directive challenged and struck down by the Court of Justice of the EU
  - National data retention laws across the EU
Session notes
An evolving harmonised approach

  - The Charter of Fundamental Rights (made binding law)
  - Development of EU data protection law
### Session notes

**An evolving harmonised approach**

- **2016**: The General Data Protection Regulation (GDPR) (became enforceable in 2018)
  - EU
  - Successor to the Data Protection Directive (Recital 171; Articles 94, 99)
Module 1: Data protection laws

EU institutions

- European Council
  - Defines EU’s priorities and sets political direction

- European Commission
  - Implements EU decisions and policies

- Council of the EU
  - Legislative decision-making

- European Parliament
  - Legislative development, supervisory oversight of the other institutions and budget development

Session notes

EU institutions

- EU comprises legislative, policy-making and judicial bodies
- European Council
  - Heads of state or government of all EU countries, European Council president, European Commission president, and High Representative for Foreign Affairs and Security Policy
  - Defines EU’s priorities and sets political direction
- European Commission
  - One commissioner per member state who pledges to respect the EU Treaties
  - Implements EU’s decisions and policies
  - Other broad functions, including executive competence to propose legislation
  - Historically most active EU institution in data protection
- Council of the EU
  - One minister from each member state—changes based on the policy issue to be discussed
  - Legislative decision-making (along with the Parliament)
  - Legislation generally proposed by the Commission before being examined by the Council of the EU and the Parliament
- European Parliament
  - Only EU institution whose members are directly elected
  - Primary responsibilities—legislative development, supervisory oversight of the other institutions and budget development
  - Greatest impact on data protection and privacy issues through role in legislative process
  - Frequent advocate for right to data protection
  - Co-decision Procedure: process by which Council of the EU and European Parliament agree on legislation
Session notes

This graphic illustrates the flow of power across EU institutions. Use the GDPR as a prime example to briefly describe the EU’s legislative process.

- The European Commission proposed the draft legislation in 2012 and sent a version to the European Parliament and the Council of the EU.
- The European Parliament reviewed the draft within committee meetings. They collected thousands of comments/amendments, and that became the European Parliament’s position on the new GDPR.
- Meanwhile, the Council of the EU had their own committees that reviewed the draft legislation. That became the Council’s official position on the new draft.
- The Parliament and Council got together and tried to jointly agree on the legislation. The European Commission adjudicated the proceedings. This process was called the Trilogue Procedure.
- Meanwhile, other groups, such as national parliaments, consumer advocates, and industry advocates, were also expressing their views.
- In December 2016, the EU Parliament and Council finally agreed upon the EU General Data Protection Regulation, first proposed in 2012; it went into effect on 25 May 2018.
- The European Court of Justice (ECJ) is the judicial body of the EU. It may be involved in cases related to data protection that begin in national courts and are referred to the ECJ for a preliminary ruling on issues of interpretation of EU law.
Pop quiz
Which role best describes the European Commission?
• Defines EU priorities and sets political direction
• Implements EU decisions and policies
• Is engaged in legislative decision-making
• Has supervisory oversight of the other institutions

Chat: Pop quiz
Which role best describes the European Commission?
• Defines EU priorities and sets political direction
• Implements EU decisions and policies
• Is engaged in legislative decision-making
• Has supervisory oversight of the other institutions
Session notes

In every member state, each country inevitably has some local differences in the law. The result is 31 laws that all broadly say the same thing but have slight differences. The GDPR was intended to eliminate those differences. However, about 50 provisions in the GDPR allow for local law clarification/exception. Whether or not the GDPR was a radical change depended on how similar your country’s data protection law was to the GDPR.

Data Protection Directive
- Directive similar to cloning yet with variances
- Obligations were on member states
- Member states’ governments implemented the Directive into local law
- Directive was transposed into national laws in EU
- Local laws/implementation differ across member states

GDPR
- Directly applicable and enforceable as law in every EU member state
- Goal is to provide just one set of data protection rules for all EU member states
- However, 50 provisions allow for local law clarification or exception
- National laws either repealed or amended to align with GDPR
- European Data Protection Board (EDPB) replaced the WP29 in 2018—to be discussed later in the training; WP29 GDPR guidelines endorsed by the EDPB
- IAPP “EU Member State GDPR Derogation Implementation Tracker”: [https://iapp.org/resources/tools/eu-member-state-gdpr-derogation-implementation](https://iapp.org/resources/tools/eu-member-state-gdpr-derogation-implementation)
Session notes

The ePrivacy Directive is discussed in more depth in Module 8.

- Processing that triggers the material scope of both:
  - ePrivacy Directive: electronic communications service, electronic communications network, and service and network publicly available and offered in the EU; website operators (e.g., for cookies) or other businesses (e.g., for direct marketing)
  - GDPR: ‘any form of processing of personal data, regardless of the technology used’

- Interplay
  - ‘To particularise’ (*lex specialis* principle): ‘Special provisions prevail over general rules’
  - ‘To complement’: Several ePrivacy Directive provisions complement GDPR provisions
  - Article 95 of the GDPR: The aim is ‘to avoid the imposition of unnecessary administrative burdens upon controllers who would otherwise be subject to similar but not quite identical administrative burdens’
  - Co-existence: In cases where *lex specialis* does not apply, the general rule will apply (*lex generalis*)

- Competence, tasks and powers of data protection authorities: ‘When the processing of personal data triggers the material scope of both the GDPR and the ePrivacy Directive, data protection authorities are competent to scrutinise the data processing operations which are governed by national ePrivacy rules only if national law confers this competence on them, and such scrutiny must happen within the supervisory powers assigned to the authority by the national law transposing the ePrivacy Directive’

Examples

- Processing that triggers the material scope of both the GDPR and ePrivacy Directive
  - Article 29 Working party’s opinion on online behavioral advertising: ‘If as a result of placing and retrieving information through the cookie or similar device, the information collected can be considered personal data’

- Interplay
  - ‘To particularise’: ‘The full range of possible lawful grounds provided by Article 6 GDPR cannot be applied by the provider of an electronic communications service to processing of traffic data, because Article 6 ePrivacy Directive explicitly limits the conditions in which traffic data, including personal data, may be processed’
  - Article 95 of the GDPR: Personal data breach notification obligations
Review question

NOTE: Review questions are intended to help reinforce key topics covered in the module. They are not meant to represent actual certification exam questions.

1. Which of the following data protection milestones is a treaty amongst member states of the Council of Europe?

   A. Data Retention Directive
   B. Charter of Fundamental Rights
   C. Convention 108
   D. ePrivacy Directive
   E. GDPR
2. Which of the following data protection milestones applies to public electronic communications services and networks?

A. Data Retention Directive
B. Charter of Fundamental Rights
C. Convention 108
D. ePrivacy Directive
E. GDPR
Review question

3. The European Convention on Human Rights is a product of which institution?

A. The United Nations
B. The Council of Europe
C. The European Union
D. The European Economic Area
4. Which role best describes the European Parliament?

A. Defines EU priorities
B. Sets political direction
C. Implements EU decisions and policies
D. Is engaged in legislative development
Module 2: Personal data

Learning objectives

• Differentiate between personal, anonymous and pseudonymous data
• Recognise special categories of data
Session notes

Four-step test: ‘Any information relating to an identified or identifiable natural person (“data subject”)’ (Article 4[1])

The criteria do not have to be considered in any particular order, yet all must be met.
Session notes

Anonymous data (Recital 26)

- Not related to an identified or an identifiable natural person
- Has been rendered unidentifiable
- Not considered personal data under the GDPR
Session notes

**Pseudonymous data** (Recitals 26, 28-29; Articles 4[5], 6[4][e], 25[1], 32[1][a])

- Not fully anonymous
- A process that detaches the aspects of the data attributed to a specific individual
- A security measure that makes the use of the data less risky
- Subject to data protection law
Chat: Knowledge check
Can you rewrite the following statement to anonymise the personal data?

Mr. Weber, CEO of Munich Ltd., earns €10,389,290.89.
Session notes

Sensitive data/special categories

• Type of personal data
• Its processing has a more profound impact on individuals’ privacy rights
• Has a higher standard of protection
• Article 9(1): ‘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’

• Personal data revealing ...
  • Racial or ethnic origin
  • Political opinions
  • Religious or philosophical beliefs
  • Or trade-union membership
Session notes

Sensitive data/special categories

• For the purpose of uniquely identifying a natural person ...
  • Genetic or biometric data
Personal data

Sensitive data/special categories

Data concerning ... health, sex life or sexual orientation

Session notes

Sensitive data/special categories

- Data concerning ...
  - Health
  - Sex life
  - Or sexual orientation
Personal data

Other

Data related to ... criminal convictions and offences
- Not considered special data, but subject to limitations on processing

Session notes

Other
- Personal data related to criminal convictions and offences
  - Article 10: Processing of such personal data ‘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’. And ‘Any comprehensive register of criminal convictions shall be kept only under the control of official authority’. 
Knowledge check

Keeping the subjective nature of this exercise in mind, provide examples that would likely belong to special categories of personal data under the GDPR.

Session notes

- A data element’s designation as belonging to a special category may not be obvious
- Example: An X-ray of a broken arm would obviously qualify as data concerning health; however, a photograph from a holiday party showing an individual with his arm in a cast may not, as the photograph does not necessarily concern that person’s health

Chat: Knowledge check

Keeping the subjective nature of this exercise in mind, provide examples that would likely belong to special categories of personal data under the GDPR.
Review question

NOTE: Review questions are intended to help reinforce key topics covered in the module. They are not meant to represent actual certification exam questions.

1. What is the function of the four-step test?

A. Determine if personal data belongs to special categories
B. Determine if personal data is anonymous
C. Determine if data qualifies as personal data
D. Determine if personal data is pseudonymous
2. Which criteria are used to identify personal data? Select all that apply.

A. ‘any information’
B. ‘relating to’
C. ‘an identified or identifiable’
D. ‘or anonymous’
E. ‘natural person’
3. Select the types of personal data elements that belong to special categories under the GDPR.

A. Personal data revealing political opinions
B. Personal data revealing religious or philosophical beliefs
C. Personal data revealing financial information
D. Genetic data used to uniquely identify a natural person
E. Data relating to personal interests and hobbies

Review question

3. Select the types of personal data elements that belong to special categories under the GDPR.

A. Personal data revealing political opinions
B. Personal data revealing religious or philosophical beliefs
C. Personal data revealing financial information
D. Genetic data used to uniquely identify a natural person
E. Data relating to personal interests and hobbies
Review question

4. True or false: Anonymising personal data is always possible.
Review question

5. True or false: Pseudonymous data is protected by the GDPR.
Review question

6. Is the collection and use of device dynamic IP addresses to allow data on a website to be transferred to the correct recipient considered personal data? Why or why not?
Module 3: Controllers and processors

Learning objectives

• Define data protection roles
• Describe basic configurations of control over personal data
Session notes

Data protection roles

- Basic definitions (not GDPR-specific)
- **Data subject:** An individual about whom personal data is processed
- **Data controller:** An organisation or individual that decides how and why personal data is processed
- **Data processor:** An organisation or individual that processes information on behalf of the data controller
- **Data protection authority (DPA), referred to as supervisory authority (SA) in GDPR:**
  - An entity appointed to enforce privacy or data protection laws and regulations in a particular jurisdiction
- GDPR-specific definitions of these roles explored throughout the course
Chat: Pop quiz

Jim is employed by a construction company in Belgium. The Human Resources department at the construction company keeps Jim’s personal data on file. The construction company contracts with a payroll company that directly deposits Jim’s paycheck into his bank account. The Belgian Privacy Commission provides regulatory oversight to ensure Jim’s company follows EU and national data protection laws.

Who is the data processor in this scenario?
Controller

Definition

- Article 4(7): ‘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’

Session notes

Article 4(7)

- Natural or legal person, public authority, agency or other body
  - Human being
  - Or legal entity
- Alone or jointly with others (see following slides)
  - Different configurations of control
- Determines the purposes and means of processing
  - Why? (purposes)
  - How? (means)
  - What data?
  - How long? (retention)
  - Where? (storage and data transfers)
  - By whom?

Following slides will define ‘joint controller’ and ‘processor’.
Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. 
(Article 26)

Session notes

Article 26 of the GDPR specifies obligations for controllers that jointly determine the purposes and means of processing personal data.

- ‘In a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation’
  - Data subject rights
  - Data subject access requests
  - Contact point for data subjects
  - ‘Essence of the arrangement’ available to data subjects
- Data subjects may exercise their rights against either controller, ‘irrespective of the terms of the arrangement’

The following slide will discuss definitions of joint controller.
Session notes

Which examples illustrate a controller determining the means and purposes of processing ‘jointly with others’?

- Scenario A
  - Group of companies: Two or more group entities determine together the purpose and means for the same processing
  - Joint responsibility
  - Separate data
  - Shared technical database/infrastructure used for individual purposes (e.g., internet-based common platform)

- Scenario B (Processor obligations are discussed on the following slide)
  - Disclosure to an internal or external processor
  - Respective rights and obligations of controller and processor

- Scenario C
  - The database for the prize draw is shared between both organisations
  - Joint responsibility

- Scenario D
  - Personal data shared from one controller to another controller (disclosure to a third-party controller)
  - Each party responsible for its own processing of the data

The EDPB Guidelines 07/2020 on the concepts of ‘controller’ and ‘processor’ may serve as a helpful resource for determining if a controller operates ‘jointly with others’. The EDPB Guidelines are available at: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf
Session notes

Processor definition

- Acts on behalf of the controller (Article 4(8))
- Processes on written instructions only (Article 28)
  - Obtains authorisation
- Provides a service to the controller (Article 28)
  - Assists the controller
  - Informs the controller of GDPR infringements
- Protects personal data (Article 28)
  - Ensures confidentiality
  - Ensures appropriate technical and organisational measures
- Demonstrates compliance (Article 30)
  - Keeps a record of processing activities on all categories of personal data processing carried out on behalf of the controller
- Enhanced obligations under the GDPR

The GDPR enhances processors’ duties and liabilities. (Yet the burden for data protection still rests heaviest on the controller.)

The role of processor is specific to the processing operation: you can be a controller for one particular processing operation, a processor for another, and so on.
If a processor infringes this Regulation by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing (Article 28).

Session notes

A processor that ‘determines the purposes and means of the processing’ (Article 4[7]) may be a controller in fact when determining the controller, the act of making processing decisions (although not necessarily lawful) can trump law and contract.

Case study

SWIFT (example of factual controller)

Following September 11, 2001, the United States Department of the Treasury served administrative subpoenas on the Society for Worldwide Interbank Financial Telecommunication (SWIFT), which required SWIFT to transfer personal data. SWIFT’s decision to transfer the data designated it as the controller, even though its contractual designation was processor.
Session notes

The GDPR’s requirements for vendor risk management may seem straightforward; however, translating its requirements into practical action points may pose challenges for the following reasons:

- Determining the extent to which the controller can rely upon the processor to attest and monitor its own reliability
- Determining the extent to which the controller needs to evaluate third parties before and after contracting, including conducting audits
- Complex contractual provisions
- Negotiating contracts between two parties of unequal bargaining power or from EU and non-EU jurisdictions
- Situations that involve cloud computing; difficulties knowing the precise nature of data processing operations at any given moment in time

A checklist may provide issues to consider at the pre-contractual due diligence stage and evidence that the necessary steps were taken. See the following slide for more details.
Session notes

- GDPR obligations on processors
  - Accountability (e.g., record-keeping, appointing data protection officer where applicable)
  - Data subjects’ rights

Engaging processors: controller pre-contractual due diligence

- Controller must ensure processors implement appropriate technical and organisational measures to secure data
- Security prioritised from beginning of controller relationship with potential processor
- Ensure enough controls to protect data shared with processor
Session notes

Controller-processor contracts (Article 28)

- If a controller is engaging a data processor, the controller is obligated to have a documented contract in place that contains:
  - Subject matter, duration and nature of the data processing
  - Types of personal data and categories of data subjects
  - Obligations and rights of the controller
  - The processor’s responsibilities
Session notes

Engaging processors: contractual terms (Article 28)

- Process personal data only on documented instructions from controller
  - Including international data transfers
- Ensure persons authorised to process personal data have committed themselves to confidentiality
  - Or are under statutory duty of confidence (i.e., processor’s employees sign NDAs)
- Implement appropriate technical and organisational measures
- Seek controller consent to engage processors
  - And flow down all terms of contract with controller to sub-contractor
- Assist controller in reporting and notifying supervisory authorities and affected individuals of data breaches
- Assist the controller in responding to requests for exercising data subject rights
- Delete or return all personal data if instructed by controller
- Make available to controller all information necessary to demonstrate GDPR compliance
- Be prepared to submit to audits, including inspections
  - By controller or another auditor chosen by controller
1. True or false: A data controller may be a natural person or a legal entity, while a data processor must be a legal entity.

**Review question**

NOTE: Review questions are intended to help reinforce key topics covered in the module. They are not meant to represent actual certification exam questions.

1. True or false: A data controller may be a natural person or a legal entity, while a data processor must be a legal entity.
Review question

2. True or false: A contract protects a processor from being held to the same legal obligations as the controller.
Review question

3. True or false: A processor may decide where and how to process personal data.
Review question

4. What actions can a controller take to manage vendor risk?
Module 4: Processing personal data

Learning objectives

• List operations in the data-processing life cycle that constitute data processing
• Describe the seven data-processing principles, especially as they relate to determining the purposes for processing
• Determine the application of the GDPR based on territorial and material scope
• Determine if a data-processing activity is legal under the GDPR based on legitimate processing criteria
Session notes
To convey the scope of data processing rules and regulations, first define data processing.
- Much more than just collecting personal data
- Article 4(2): ‘Any operation’ performed upon data
Session notes

GDPR Principles for processing

- Article 5
- Carried over from earlier laws and regulations, including OECD Guidelines
- May be broadly interpreted; however, violators may incur large administrative fines

- **Lawfulness, fairness and transparency of processing:** Honest practices, such as communicating openly with data subjects about personal data processing activities

- **Purpose limitation:** Collecting and processing personal data for the specified purpose only
  - To determine if personal data may be processed further, use a compatibility test to look for links between purposes, nature of the data, method of collection, consequences of secondary uses and safeguards

- **Data minimisation:** Processing only personal data that is relevant and necessary for the purpose

- **Data quality and accuracy:** Processing complete and up-to-date personal data

- **Storage limitation:** Retaining only personal data that is relevant and necessary for the purpose

- **Integrity and confidentiality:** Ensuring personal data is secure

- **Accountability:** Processing personal data responsibly and demonstrating compliance with EU and member state data protection laws
Session notes

Denmark DPA recommends GDPR fine for taxi company (2019)

Denmark’s data protection authority, Datatilsynet, recommended a fine of $180,000 to taxi company Taxa 4x35 for violations of the GDPR, Bloomberg Law reports. The DPA found the taxi company did not adhere to the GDPR’s data-minimisation principle. While Taxa deleted the names from all its records after two years, the rest of the ride records remained intact. The DPA recommended the fine after it was discovered the taxi company continued to hold onto individuals’ phone numbers after their names were removed from the records.
Session notes

Dutch DPA hits tennis association with 525K euro GDPR fine (2020)

Sponsors of the Royal Dutch Lawn Tennis Association (KNLTB) received personal data in the form of names, genders and addresses from the association for the purpose of marketing tennis-related and other offers to KNLTB members. The Dutch Data Protection Authority served the KNLTB with a 525K euro fine declaring that the association did not have any basis under the GDPR data processing principles for sharing personal information of its members with sponsors. The KNLTB states that the data sharing was based on legitimate interest under the GDPR and has objected to the fine.
An access control system used for building security is later used to pull login data to track employee punctuality. The employees are not informed of this new processing action, and the controller does not keep consistent records of the processing activities.

Which GDPR principles may have been violated?
Processing personal data

Territorial scope of the GDPR: Three criteria

1. Processing of personal data where a controller or processor is established in the EU

Session notes

The GDPR lays out specific criteria for its application, which covers territorial and material scope (material scope covered later in this module).

Territorial scope relies on three criteria as set out in Article 3 of the GDPR. Just one of these criteria must be met for the GDPR to be applicable.

1. Processing of personal data where a controller or processor is established in the EU (regardless of whether or not the actual processing takes place in the EU)
   - EDPB guidance: A processor is not necessarily an establishment of a controller based on its status of processor alone
Processing personal data

Territorial scope of the GDPR: Three criteria

1. Processing of personal data where a controller or processor is established in the EU

2. Processing of personal data of data subjects in the EU relating to offering goods or services or monitoring behaviour in the EU

Session notes

The GDPR lays out specific criteria for its application, which covers territorial and material scope (material scope covered later in this module).

Territorial scope relies on three criteria as set out in Article 3 of the GDPR. Just one of these criteria must be met for the GDPR to be applicable.

2. Processing of personal data of data subjects in the EU relating to offering goods or services or monitoring behaviour in the EU (where the controller or processor is not established in the EU)
   
   - Data subject-centric way of determining applicability of the law
   - EDPB guidance: Processing personal data of individuals in the EU alone is not the trigger; the important element is ‘targeting’
   - Offering of goods and services to data subjects residing in the EU (a website directed at the relevant jurisdiction)
   - Monitoring
     - Digital tracking of behavior
     - EDPB guidance: plus CCTV usage and market surveys
     - A ubiquitous practice
     - EDPB guidance: not just any online collection or analysis of personal data, but dependent on purpose
Session notes

The GDPR lays out specific criteria for its application, which covers territorial and material scope (material scope covered later in this module).

Territorial scope relies on three criteria as set out in Article 3 of the GDPR. Just one of these criteria must be met for the GDPR to be applicable.

3. Processing of personal data by a controller not established in the EU but in a place where member state law applies by virtue of public international law
**Material scope:** ‘processing of personal data wholly or partly by automated means’ or ‘processing other than by automated means of personal data which form part of a filing system’ (Article 2)

**Session notes**

**Material scope** (Article 2)

- ‘Processing of personal data wholly or partly by automated means’
  - Any processing operation performed without or partly without human intervention
  - No to be confused with automated decision-making, which has strict restrictions under the GDPR (discussed in Module 5)

- ‘Personal data which forms part of a filing system’
  - Or are intended to form part of a filing system
  - Even if the processing is not conducted by automated means

**Exclusions**

- Activities outside the scope of EU law (e.g., national security activities)
- Law enforcement and public security
- Purely personal or household activities
Case study


Mrs. Lindquist (whose purposes were mostly charitable and religious) published on a private home page personal data about her colleagues, including telephone numbers and information about a coworker’s injured foot and medical leave. This case raised the question if a private home page accessible to only those who have the address is permitted under one of the exclusions (household activity). The Court of Justice of the EU ruled that it is not.
Session notes

Lawful grounds (Article 6)

- If activities fall within the territorial and material scope of the GDPR ...
- One of six conditions must be met
- Consent from the data subject for a specific processing purpose
  - Commonly used
  - However, under the GDPR additional conditions must be met
- Conditions for consent
  - Demonstrable (if processing based on consent)
  - If a written declaration, clearly distinguishable, etc.
  - Right to withdraw any time (as easy as it was to give)
  - Not conditional for performance of contract if not necessary
Session notes

Lawful grounds (Article 6)

- Performance of a contract
  - If the processing is necessary to perform the contract (and the data subject is a party to the contract)
  - Or if the data subject requests the processing in order to enter into a contract
Session notes

Lawful grounds (Article 6)
- Compliance with a legal obligation to which the controller is subject
  - Meant to be interpreted narrowly
  - Applies to legal obligations required by EU and member state laws only
  - Does not include legal obligations of contracts or those of third countries (outside the EU)
**Session notes**

**Lawful grounds** (Article 6)

- Protection of *vital interests* of the data subject or another natural person
  - If personal data must be processed to ensure an individual’s survival
  - Should only be used in an emergency situation and if no other option is available
Session notes

Lawful grounds (Article 6)

- Necessary for the public interest or in the exercise of official authority of the controller
  - Controller required to process personal data in the public interest
  - Member state legislation may determine what tasks fall within the public interest
**Processing personal data**

Lawful grounds for controllers

- Consent
- Contractual necessity
- Legal obligation
- Vital interests
- Public interest
- Legitimate interests

**Session notes**

**Lawful grounds** (Article 6)

- Necessary for the legitimate interests of the controller or a third party (unless overridden by the interests, rights or freedoms of the data subject, in particular where the data subject is a child)
  - Has often been used as a safety net in the absence of another legitimate basis for processing personal data
  - While it may still prove a more realistic option than consent, it should be used with caution
Processing personal data

Consent

• Clear affirmative act
• Freely given
• Specific and informed
• Unambiguous
• Indication of wishes
• Written, electronic, oral or any other means
• Conditions


Session notes

Consent has always been one of the cornerstones of EU data protection; however, under the GDPR, the conditions for consent have become elevated.

The elevated requirements for consent have made it difficult to obtain lawfully.

Consent (Recitals 32, 42-43; Articles 4[11], 7)

• Freely given
  • Not if service is conditional on consent
  • Not if there is a clear imbalance of power between the data subject and the controller
  • As easy to withdraw as it is to give
• Specific
  • For all purposes
• Informed
  • Clearly distinguishable from other matters
  • Intelligible
  • Clear and in plain language
  • Compatible with the original purpose
• Unambiguous
  • Absolutely clear
• Indication of wishes
  • Clearly an affirmative action (e.g., opt-in, technical setting for information society services, browser setting)
  • Not silence, inactivity, a pre-ticked box or opt-out
  • Implied through the provision of data
• Conditions for consent
  • Demonstrable (if processing based on consent)
  • If a written declaration, clearly distinguishable, etc.
  • Right to withdraw any time (as easy as it was to give)
  • Not conditional for performance of contract if not necessary
Chat: Pop quiz
Fill in the blank: Consent must be ____ .
**Processing personal data**

Consent for children’s data

- Information society services
- Authorisation of parent or guardian of children below 16 years old
- Reasonable efforts to verify

---

**Session notes**

Obtaining consent for processing children’s personal data

- Even more rigorous when information society services are being offered
  - Including online technologies (e.g., social media and apps)
- Consent must be given by a parent or guardian when the child is younger than 16 years old
  - Member states can lower threshold to as young as 13 years old
- Controller must make reasonable efforts to verify
Brainstorm

Methods a controller may use to verify parental authorisation

Session notes

- Think about the children you know and all the online technologies they use (and how often)
- Imagine the difficulty for parents to consent to every service a child uses online, including social media and apps

Chat: Brainstorm

Methods a controller may use to verify parental authorisation
**Processing personal data**

**Legitimate interests**

- Processing is necessary
- Interests are balanced against the data subject's
- Criteria is more restrictive

---

**Session notes**

**Legitimate interests** of the controller or third party (Recitals 47–49)
- **Processing is necessary** to meet the controller or third party’s legitimate interests
- **Interests are balanced against the data subject’s** (balancing test)
- An attractive alternative to consent, yet no longer a fallback option
- **Criteria is more restrictive**
  - Compliance with other legal obligations
  - Transparency
  - Economic interests not necessarily sufficient
  - Importance of upholding fundamental rights and freedoms of the data subjects
  - Use limitation: compatibility
  - Adequate safeguards for secondary uses, including pseudonymisation and encryption
Session notes

- Explicit consent
  - Unambiguous, freely given, specific and informed, and a clear affirmative act by the data subject
- In the context of employment
  - When the processing of special categories is necessary for the controller to comply with a legal obligation under employment, social security and social protection law
  - When data subjects are candidates, employees, contractors
- Vital interests of individual
  - Controller must be able to demonstrate that it is not possible to obtain consent
- Political, philosophical and religious purposes
  - Covers particular foundations, associations, not-for-profit bodies and any foundation, association or not-for-profit body with trade union aim
  - Relates to the processing of special categories of data about members of the organisation, former members or those who have regular contact with the organisation for the organisation’s purposes
  - Appropriate safeguards in place to protect personal data
  - The data must not be disclosed outside the organisation without the data subject’s consent
- Sensitive data manifestly made public by the data subject
  - When data subjects disclose sensitive data about themselves (e.g., details about political opinions or health while giving a media interview)
  - Data collected from social networking sites
### Session notes

- **Establishment, exercise or defence of legal claims**
  - Controller must establish necessity
  - Close and substantial connection between the processing and the purpose

- **Substantial public interest**
  - Narrower under GDPR
  - Reason for processing balanced with data subject’s right to data protection
  - Suitable and specific measures to safeguard data subject’s fundamental rights and interests
  - Member states can specify reasons of public interest (e.g., preventing and detecting crime)

- **Medicine and social healthcare**
  - Assessing the working capacity of an employee, making a medical diagnosis, providing health or social care or treatment, managing health or social care systems or services
  - Reason for processing based on EU or member state law, or necessary to fulfil a contract

- **Public health**
  - Based on EU or member state law
  - GDPR examples: ‘Protecting against serious cross-border threats to health or ensuring high standards of quality and safety in health care and of medicinal products or medical devices’

- **Public archives or scientific or historical research or statistical**
  - Further interpretation from member state law
  - Processing proportionate to the purpose
  - Suitable and specific measures to safeguard data subject’s fundamental rights and interests
Review question

NOTE: Review questions are intended to help reinforce key topics covered in the module. They are not meant to represent actual certification exam questions.

1. What is data processing?

A. Any action involved in collecting personal data
B. Any action performed upon data
C. Any action involved in securing and protecting data
D. Any action that adapts or alters data
2. What are the criteria used to determine the territorial scope of the GDPR? Select all that apply.

A. Processing of personal data when a controller or processor is established in the EU
B. Processing of personal data of EU subjects relating to offering goods or services or monitoring behaviour
C. Processing of personal data by a controller not established in the EU but in a place where member state law applies
3. True or false: Exclusions to the material scope of the GDPR should be interpreted broadly.
Review question

4. Which exception to the prohibition on processing special categories of data must be explicit?

A. Consent
B. Vital interests
C. Publicly available data
Learning objectives

- Describe data subjects’ rights regarding the processing of their personal data
- Recognise controller and processor obligations regarding data subjects’ rights
Data subjects’ rights

Access

• Confirmation of processing and access
• Processing information
  - Purpose
  - Categories of personal data
  - Recipients
  - Retention period
  - Additional data subject rights
  - Source of personal data
  - Automated decision-making
• Appropriate safeguards for data transfers
• A copy of the personal data

Session notes

(Recitals 59, 63; Article 15):
Data subjects shall have the right to:

• **Confirmation** their personal data is being processed and **access** to it
• **Processing information**
  • **Purpose** of the processing
  • **The categories of personal data**
  • **Recipients**/categories of recipients of the personal data, in particular in third countries/international organisations
  • **Retention period**/criteria used to determine period
  • Information about **data subject rights** to rectification, to erasure, to restriction, to object and to lodge a complaint with an SA
  • Any available information about the **source of the personal data** (when not collected from the data subject)
  • The existence of **automated decision-making** and information about:
    • The logic involved
    • Significance and envisaged consequences
• Information about **appropriate safeguards for personal data transferred** to a third country/international organisation
• **A copy of the personal data** being processed from the controller
  • Controller may charge reasonable fee for further copies requested
  • Commonly used electronic form when the request is made by electronic means (and unless otherwise requested)
  • Cannot adversely affect the rights and freedoms of others
Session notes

**Rectification** without undue delay (Article 16)

- Data subjects shall be able to correct or complete their personal data
- **Correction** of inaccurate personal data
- **Completion** of incomplete data (with consideration for the processing purpose)
- Where the data must be saved, the data subject may submit a supplementary statement
Brainstorm
Under what circumstances might a data subject want or need personal data with an error to be saved?

Chat: Brainstorm
Under what circumstances might a data subject want or need personal data with an error to be saved?
Data subjects’ rights

Limitations

• Identification of the requester
• Protection of others’ rights and freedoms
• Purpose of the request
• Manifestly unfounded or abuse of right

Session notes

Limitations to rights of access and rectification

• Identification of the requester
  • With reasonable steps to identify
• Protection of others’ rights and freedoms, including data controller (e.g., trade secrets and intellectual property)
• Purpose of the request
  • To check the lawfulness of processing and accuracy of personal data
• Request is manifestly unfounded or excessive
  • Repetitive character
Chat: Brainstorm

Scenarios that may limit a data subject’s rights to access or rectification
Session notes

**Data portability** (Article 20)
- Applies where consent or performance of a contract is used as lawful grounds for processing
- Extension of access right
- Structured, commonly used and machine-readable format
- **Interoperability**: accessibility through multiple systems (Recital 68)
  - As much metadata as possible
  - Does not mean maintaining compatible systems
- Transfer to data subject (e.g., direct download), another controller (e.g., application programming interface) or a trusted third party
  - Data controller transferring the data not responsible for the processing activities of the recipient
  - Data portability does not trigger erasure
Data subjects’ rights

Data portability cumulative conditions

1. Personal data processed automatically on the basis of consent or the performance of a contract
2. Personal data concerning and from the data subject
3. Data portability does not adversely affect the rights and freedoms of others

Session notes

The Article 29 Working Party has provided ‘Guidelines on the Right to Data Portability’, which further defines this data subject right.

Data portability cumulative conditions

1. Personal data processed automatically (not paper files) on the basis of consent or the performance of a contract
2. Personal data concerning and from the data subject (including that observed from activities of the user)
3. Data portability does not adversely affect the rights and freedoms of others (e.g., a data set containing personal data relating to other individuals, as well as the individual requesting data portability)
Session notes

Right to erasure (‘right to be forgotten’) (Recitals 59, 65-66; Articles 17, 19)

- Right to have personal data erased (and no longer processed)
  - Data no longer necessary for the purpose
  - Withdrawn consent if processing is based on consent
  - Objection to processing (if processing is based on legitimate interests)
  - Data collected in relation to information society services from a child on the basis of consent
  - Unlawful processing
  - Compliance with EU and member state law

- Right to have public data deleted
  - Google Spain v. AEPD and Mario Costeja González
  - Data made public by the controller (e.g., posting a photo of an individual on a social media profile with a public setting)
  - Reasonable steps by the controller to inform other controllers that the data subject has requested erasure of links to, copies and replications of the data (Recital 66)

- Burden on the controller to remove the data
- Exceptions ... (see Article 17)
Your outlook
Regarding the right to be forgotten, what difficulties might controllers have with third-party follow-up?

Chat: Your outlook
Regarding the right to be forgotten, what difficulties might controllers have with third-party follow-up?
Session notes

**Restriction of processing** (Article 18)—new right under GDPR
- **Definition**: Personal data is stored without being further processed
- **Circumstances**: When storing data ...
  - Is legally required
  - Ensures protections of another’s rights
  - Is in the public interest
- **Reasons** data subjects may request restriction
  - Accuracy is contested and controller needs time to verify
  - Processing is unlawful, but data subject prefers restriction to erasure
  - Controller no longer needs data, but data subject needs it for establishment, exercise or defence of legal claims
  - Data subject objects to processing, pending controller’s verification of legitimate grounds
- Once restricted, data may only be **further processed**...
  - With new consent from the data subject
  - To exercise or defend legal claims
  - To protect the rights of another person
  - For important public interest reasons
- Controller must inform data subject before **lifting the restriction**
Session notes

Right to object to processing (Article 21)

- Three sub-categories
  - Public interest or legitimate interest
    - Not an absolute right
    - Data subject’s right to object at any time to processing based on the public interest or the controller’s legitimate interest
    - Controller burden to demonstrate compelling, legitimate interest that overrides individual’s interests, rights and freedoms
Session notes

**Right to object to processing** (Article 21)

- Not an absolute right
- Three sub-categories
  - **Research or statistical purposes**
    - Data subject’s right to object at any time to processing for scientific/historical research or statistical purposes
    - On grounds relating to individual’s particular situation
    - Overridden if processing is necessary for performance of a task carried out in the public interest
**Data subjects’ rights**

Right to object to processing

- Public interest or legitimate interests
- Research or statistical purposes
- Direct marketing

### Session notes

Right to object to processing (Article 21)

- Not an absolute right
- Three sub-categories
  - Direct marketing
    - Data subject right to object at any time to processing for direct marketing purposes
    - Absolute
    - Must cease processing
    - Includes profiling
The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her (Article 22).

**Session notes**

(Recital 71; Article 22)

**Prohibition on:**
- A decision based solely on automated processing
  - And produces legal or otherwise similarly significant effects
- “Solely automated process” and which decisions have “significant effects on individuals” needs guidance from regulator
- Strictest for decisions involving children

**Exemptions (all requiring appropriate safeguards):**
- Processing necessary to enter into or perform a contract (e.g., evaluating credit risk or insurance risk)
- Authorisation of member state law
- Data subject’s explicit consent

**Automated decision-making not permitted on special categories of personal data, unless:**
- Explicit consent
- Or substantial public interest based on union or member state law
- Suitable measures must be put in place

**Article 29 Working Party good practice recommendations:**
- Provide ‘meaningful information about the logic involved’
- If relying on consent, consult the WP29 guidelines on consent
- Consider implementing a mechanism for data subjects to check profiles and allow them to amend inaccuracies
- Explicitly bring to the attention of the data subject the right to object, clearly and separately from other information
- Use appropriate safeguards (e.g., regular quality assurance checks to systems to make sure individuals are treated fairly and not discriminated against); additional safeguards in guidance
**Data subjects’ rights**

**Profiling**

- Automated processing
- Of personal data
- To evaluate, analyse and predict
- Personal aspects
- Relating to a natural person

**Session notes**

**Profiling** (Articles 4[4], 22)

- Automated processing
- Of personal data
- For the purpose of evaluating, analysing and predicting
- Personal aspects
- Relating to a natural person

Examples of behavioural profiling/targeting:

- **Adware**
  - Software installed on a user’s computer
  - Often bundled with freeware
  - Monitors online behaviour to target advertising to the user
- **Web cookie**
  - Piece of text that web server can store on user’s computer hard disk
  - Later retrieves to get information about user
- **Web beacon**
  - Passes information from user’s computer to third-party website
  - Delivered through browser or email
  - Used to build profiles of user behaviour
  - Commonly used for online ad impression count, file download monitoring, ad campaign performance and monitoring email reading
- **Digital fingerprint**
  - Can identify end-user device based on information revealed as part of web page request
Chat: Your outlook

Under what circumstances may profiling be considered an invasion of privacy?
Review question

NOTE: Review questions are intended to help reinforce key topics covered in the module. They are not meant to represent actual certification exam questions.

1. Which of the following data subjects’ rights provides data subjects with entitlements to certain information, obtainable from the controller upon request?

   A. Right to restriction of processing
   B. Right of access
   C. Right to erasure
   D. Right to object
2. The right of access grants data subjects' access to which of the following types of information? Select all that apply.

A. The purpose of the processing
B. Retention periods
C. The means of data storage
D. Recipients of the personal data
Review question

3. Which is not listed by the GDPR as a method for restricting processing of personal data?

A. Noting the restriction in the system
B. Moving the data to a separate system
C. Temporarily removing published data from a website
D. Disabling the data management system
Review question

4. Under which categories may a data subject object to processing personal data? Select all that apply.

A. Establishment, exercise or defence of legal claims
B. Direct marketing
C. Public interest or legitimate interest
D. Research or statistical purposes
5. What is profiling?

A. The processing of personal data gathered from social media sites
B. A form of automated decision-making
C. The act of enabling cookies
D. All the above
Module 6: Information provision obligations

Learning objectives

• Define transparency as it relates to the controller’s communications with the data subject
• List the information that should be provided by the controller to the data subject when personal data is collected both directly and indirectly
Session notes

Transparency

  - ‘Transparency is an overarching obligation under the GDPR applying to three central areas: (1) the provision of information to data subjects related to fair processing; (2) how data controllers communicate with data subjects in relation to their rights under the GDPR; and (3) how data controllers facilitate the exercise by data subjects of their rights’
- Data controllers are to communicate with individuals using ...
  - An intelligible and easily accessible form
    - Article 12(1): ‘The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally’.
    - Free of charge unless request is unfounded or excessive
Session notes

Transparency

- Data controllers are to provide notice using ...
  - Clear and plain language
    - Adapted to the data subject
    - Especially for children
Session notes
Transparency
  • Data controllers are to provide notice using ...
    • **Concise** communication
Chat: Your outlook
What are the challenges around making information accessible, clear and concise?
Session notes

Privacy notice

- A statement made to a data subject that describes how the organisation collects, uses, retains and discloses personal data
- Related terms: privacy statement, fair processing statement, privacy policy
- Large volume of required information = creative methods for communication
Chat: Share your experience
What strategies does your organisation use to make its privacy notices easy to navigate and concise?
Session notes

Transparency strategies

• For making privacy notices easier to navigate and more concise

• Layered privacy notice
  • Multiple layers of increasingly detailed notices
  • The Article 29 Working Party endorsement of up to three layers (so long as the sum total meets legal requirements)
  • Top layer: short notice—just key elements with links
  • Second and third layers
    • Condensed notice followed by a full notice
    • Or full notice followed by FAQs and additional links

• ‘Just-in-time’ notice
  • Delivered at or right before a user accepts a service or product
  • Or when previously collected data is to be used for a new purpose
  • Helps to facilitate meaningful choice

• Standardised icons (Article 12[7])
  • Visualisation
  • Challenge: to design readable icons
  • European Commission
When to notify

Controllers are required to provide data subjects with information about processing prior to collection.

- Not always possible if obtained from indirect source (e.g., public records)
- Prior to further processing
- Article 13: Notice not required if data subject already has information
Let’s talk about...
What information must be provided to data subjects for direct collection vs. indirect collection of personal data?

Chat: Let’s talk about...
What information must be provided to data subjects for direct collection vs. indirect collection of personal data?

**Direct collection**
- Identity and contact details of the controller and data protection officer
- Purpose and legal basis of processing
- Recipients of the personal data
- Intention to transfer data to a third country or international organisation
- Legal basis for intended international transfers, including the fact that either the receiving country has an adequacy decision from the Commission or other appropriate safeguards are in place, as set out in Articles 46, 47 and 49; and how to obtain a copy of these safeguards
- Legitimate interests of the controller if the controller uses its legitimate interests as the legal basis for the collection
- Storage period or the criteria used to determine the length of storage
- Data subjects’ rights to withdraw consent at any time, to request access, to rectification or restriction of processing, and to lodge a complaint with a supervisory authority; plus, the fact that withdrawing consent does not affect the lawfulness of processing that has already been completed if the controller uses consent as its legal basis for collection
- Whether the provision of the personal data is a statutory or contractual requirement, as well as whether the data subject is obliged to provide the data, and consequences of failing to do so
- Information about the use of automated decision-making

**Indirect collection** within a reasonable period after obtaining the data (no more than one month) or upon first communication with the data subject when personal data is used to communicate
- See above requirements
- The categories of personal data concerned
- Plus the source of the data
Exception

Subject to strict criteria to ensure the rights and freedoms of the data subject

• Data subject already has the information
• Subject to strict criteria to ensure the rights and freedoms of the data subject
  • If impossible or requires disproportionate effort
    • Example from Article 29 Working Party’s ‘Guidelines on transparency’: ‘A large metropolitan hospital requires all patients for day procedures, longer-term admissions and appointments to fill in a Patient Information Form which seeks the details of two next-of-kin (data subjects). Given the very large volume of patients passing through the hospital on a daily basis, it would involve disproportionate effort on the part of the hospital to provide all persons who have been listed as next-of-kin on forms filled in by patients each day with the information required under Article 14.’
    • If it would render impossible or seriously impair the purpose of the data processing
• If national or EU laws require obtaining or disclosing data and provide appropriate measures to protect individuals' interests
• If national or EU laws require that the personal data remain secret
Session notes
Poland’s DPA issues its first GDPR fine (2019)

Poland’s data protection authority has issued its first fine under the GDPR, TechCrunch reports. The Personal Data Protection Office fined digital marketing company Bisnode 220,000 euros for its failure to fulfil its data subject rights obligations under Article 14 of the GDPR. The DPA gave Bisnode three months to reach out to 6 million people in order to meet its Article 14 information notification requirements. ‘The decision is seen as radical, as it interprets Article 14 literally’, Oxford University Center for Technology and Global Affairs Research Associate Lukasz Olejnik said. ‘UODO has taken a very principled position, arguing that the company business model is fully based on processing scraped data, and that the company has taken a decision willingly’.
Review question

NOTE: Review questions are intended to help reinforce key topics covered in the module. They are not meant to represent actual certification exam questions.

1. True or false: A controller may charge an administrative fee to data subjects if they request that the information provision be in an oral format.
Review question

2. True or false: The transparency principle states that detail is more important than conciseness in a privacy notice.
Review question

3. What information must be provided to data subjects when the controller’s necessity is being used as the legal basis for processing?

A. Source of the data
B. Controller’s legitimate interest
C. Legal basis for transferring data internationally
D. Recipients of the data
4. What information must be provided to data subjects when the personal data that will be processed was collected indirectly?

A. Source of the data
B. Storage period
C. Controller’s legitimate interest
D. Statutory or contractual requirement
Review question

5. What information must be provided to data subjects when their personal data will be shared with an outside organisation to provide them with a promised service?

A. Intention to transfer data internationally
B. Use of automated decision-making
C. Source of the data
D. Recipients of the data
6. What information must be provided to data subjects in all circumstances? Select all that apply.

A. Purpose of processing
B. Data subjects’ rights
C. Identity of the controller
D. Controller’s legitimate interest
Review question

7. True or false: Information provision is required, even if it necessitates disproportionate effort.
Module 7: International data transfers

Learning objectives

• Define transparency as it relates to the controller’s communications with the data subject
• List the information that should be provided by the controller to the data subject when personal data is collected both directly and indirectly
Session notes

First, ensure legal basis to process personal data (discussed earlier in Module 4).

The landscape of cross-border data transfer options (discussed in more depth on following slides) should be considered in order, one through three:

1. Adequacy decisions
2. Appropriate safeguards
3. Derogations

Controller now obligated to inform data subject about data transfers

- Has always been good practice
- If controller plans to transfer personal data internationally, must tell data subject of existence or absence of adequacy decision
- Regardless of legal basis for transfer
  - Controller must inform data subject of intent to transfer personal data to another country or multinational organisation
  - Must describe safeguards being used to protect the data
International data transfers

Adequacy

• What is it?
  • Adequate level of data protection for a country, territory, sector (e.g., healthcare or financial services) and international organisation

• Who determines it?
  • The European Commission (through implementing act and examination procedure)
    • Mechanism for reviewing every four years
    • Ability to repeal, amend and suspend
    • Already existing decisions (from Directive) in force until amended, replaced and appealed

• What is the criteria?
  • Respect of rule of law
  • Access to justice
  • International human rights standards
  • General and sectoral laws and case law
  • Effective and enforceable rights for individuals, including effective administrative and judicial redress
  • Data protection rules, professional rules and security measures—including specific rules for onward transfers
  • Other international commitments or obligations

• With adequacy decision, no additional authorisation for transferring data required
Session notes

Case summary

Schrems v. Data Protection Commissioner

Mr. Schrems was a Facebook user in Austria. After revelations of NSA surveillance in the U.S. allegedly involving Facebook’s cooperation, Schrems complained to the Irish SA that Facebook Ireland, the company’s European subsidiary, was improperly transferring his data to the U.S. where it could be accessed by the NSA. The data transfers from Facebook Ireland to the U.S. were allowed under the Safe Harbor adequacy decision. However, because the European Commission had not assessed U.S. limits on government access to data for national security purposes in its Safe Harbor adequacy determination, the CJEU struck down the adequacy determination as inconsistent with the European right to privacy.

A subsequent ruling by the CJEU on July 16, 2020 invalidated the European Commission’s adequacy determination for the EU-U.S Privacy Shield, citing that:

• The U.S. surveillance programs are not limited to what is strictly necessary and proportional as required by Article 52 of the EU Charter on Fundamental Rights
• EU data subjects lack actionable judicial redress and don’t have the right to an effective remedy in the U.S., as required by Article 47 of the EU Charter
• The CJEU decision also included findings regarding the need for case-by-case assessments of the sufficiency of foreign protections when using standard contractual clauses, discussed in more detail later.
Chat: Let’s talk about...

How do the Schrems judgments raise the threshold in general for adequacy assessments?

Resources:
https://iapp.org/resources/article/guidance-notes-for-responding-to-schrems-ii/
Discuss

How are personal data transfers from the EU to the U.K. to be governed after the end of the six-month grace period included in the EU/U.K. Trade and Cooperation Agreement?

Session notes

2016: U.K. voted by narrow margin to leave EU

In January 2020, the European Parliament voted to end the U.K.’s membership in the EU. On 24 December 2020, days before the Brexit transition period came to an end, the U.K. and EU reached a comprehensive agreement known as the EU/U.K. Trade and Cooperation Agreement.

While the focus of the agreement is on trade and the movement of goods between the U.K. and European Economic Area, the agreement has implications for the privacy practices of controllers processing U.K. and/or EEA personal data.

Most significantly, the agreement foresees that during a period of maximum four months, which can be extended by another two months, EEA personal data can continue to flow freely to the U.K., notwithstanding the fact that, so far, the U.K. has not secured adequacy treatment under the EU GDPR. Conferring an adequacy decision on the U.K. will require a proposal from the European Commission, an opinion from the European Data Protection Board, approval by EU member state representatives and an adopting decision by the commissioners. The U.K. has already indicated that it considers the EU data protection regime adequate so that personal data can continue to flow freely from the U.K. to the EU.

The U.K. Data Protection Act was enacted 23 May 2018. The law replaces the Data Protection Act 1998 and sets new standards for data protection in accordance with the GDPR. The U.K. has transposed GDPR through the Data Protection Act 2018, which continues to be in force after Brexit. Consequently, the principles and rules of EU data protection law continue to apply in the U.K. Organisations subject to both the U.K. Data Protection Act and EU GDPR may also need to appoint representatives in each jurisdiction if they qualify as controllers located in a third country.

Chat: Discuss

How are personal data transfers from the EU to the U.K. to be governed after the end of the six-month grace period included in the EU/U.K. Trade and Cooperation Agreement?

Resources: Jetty Tielemans, “Updated Brexit Privacy Checklist,” IAPP Resource Center, January 2021,
https://iapp.org/media/pdf/resource_center/brexit_privacy_checklist.pdf
International data transfers

Appropriate safeguards
- Standard data protection clauses
- Approved codes of conduct and certification mechanisms
- Ad hoc contractual clauses
- International agreements

Session notes

Appropriate safeguards (Article 46)
- Approved codes of conduct and certification mechanisms (discussed on following slides)
- Binding corporate rules (discussed later in module)
- Standard contractual clauses
  - Also known as model clauses
  - Adopted by the Commission or a national SA (and then approved by the Commission)
  - For a company in EEA that wants to send data to company outside EEA
  - Different types for data controllers and processors
  - Standard form that is non-negotiable
  - Most commonly used tool for appropriate safeguards
- In the wake of “Schrems II,” the legality of SCCs was upheld. However, companies must conduct case-by-case assessments on the laws in each recipient country to ensure essential equivalence to EU law for personal data being transferred under SCCs or BCRs. If the laws are not essentially equivalent, companies must provide additional safeguards or suspend transfers. Such additional safeguards can involve additional technical controls and contractual obligations on how to manage onward transfers and compelled disclosures to authorities.

The process of assessing data protection equivalence is commonly referred to as conducting a “Transfer Impact Assessment (TIA).” Note that this is NOT terminology used by the EDPB or European Commission, but rather an industry-coined term. To facilitate this assessment, many organisations are relying on questionnaires and adopting a combination of technical, organisational and contractual safeguards.
International data transfers

Appropriate safeguards (continued)

- Standard data protection clauses
- Approved codes of conduct and certification mechanisms
- Ad hoc contractual clauses
- International agreements

Session notes

Appropriate safeguards (Article 46) continued

- Ad hoc contractual clauses
  - Must have SA authorisation
  - Allow for individual tailoring to company needs
  - Provisions for such clauses may differ at member state level

- Reliance on international agreements
  - Two countries may enter into an agreement between themselves to provide for protection of personal data
  - Example: Passenger name records (PNRs) - see https://www.dhs.gov/publication/passenger-name-records-agreements
### International data transfers

Appropriate safeguards: codes of conduct

- Created/revised by associations and other bodies representing controllers or processors for:
  - GDPR application
  - Helping controllers and processors demonstrate compliance
  - Creating market efficiencies
  - Facilitating international data transfers
- Binding and enforceable

---

### Session notes

**Codes of conduct**: compliance-signalling tools for controllers and processors (Articles 40, 41)

- **Created/revised by associations/other bodies representing controllers or processors for:**
  - GDPR application (see list of topics in Article 40)
  - Helping controllers and processors demonstrate compliance
    - Risks associated with data processing and security obligations
  - Creating market efficiencies (e.g., saving a controller from having to conduct its own review of a potential data processor’s systems and monitoring its ongoing compliance). Helps to streamline contracting and reduces time needed for internal legal review.
  - Facilitating international data transfers
    - Non-EU controllers and processors must also make ‘binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards, including as regards data subjects’ rights’

- **Binding and enforceable**
  - Approved codes of conduct must enable ‘the mandatory monitoring of compliance with its provisions’ by accredited monitoring bodies
  - When a controller or processor infringes the code, an accredited body can suspend or exclude the infringing party from the code, notifying the supervisory authority of the proceeding
  - Adherence with a code is a factor to be considered in assessing an administrative fine
International data transfers

Appropriate safeguards: certification mechanisms

• May be issued by accredited certification bodies, competent supervisory authorities and the EDPB for:
  - Assisting controllers and processors in same situations as through codes of conduct
  - Additionally, demonstrating compliance with Article 25—data protection by design and by default

• Good for no more than three years (may be renewed)

• Consequences for noncompliance

Session notes

Certifications: recognised by the GDPR (along with seals and marks) as acceptable mechanisms for demonstrating compliance (Articles 42, 43)

• ‘Shall be voluntary and available via a process that is transparent’
• Does not serve to ‘reduce the responsibility of the controller or the processor for compliance’
• May be issued by accredited certification bodies, competent supervisory authorities and the EDPB for:
  • Assisting controllers and processors in same situations as through codes of conduct
  • Additionally, demonstrating compliance with Article 25—data protection by design and by default
• Good for no more than three years (may be renewed if conditions and requirements are still met)
• Consequences for non-compliance
  • Accredited certification body responsible for withdrawing certification in the event of noncompliance
    • Must inform the supervisory authority and provide reasons
  • Certification is a factor to be considered in assessing an administrative fine
International data transfers
Appropriate safeguards: binding corporate rules

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Companies engaged in joint economic activity</td>
<td>Internal and legally binding rules</td>
<td>Standard applications</td>
<td>Flexibility</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Approval by supervisory authorities</td>
<td></td>
</tr>
</tbody>
</table>

Additional references:  
https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614109  
https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614110

Session notes
Appropriate safeguards: binding corporate rules (BCRs)

• Who
  • Companies engaged in joint economic activity
  • Corporate groups and groups of enterprises
  • Controllers and processors

• What?
  • Internal and legally binding rules
  • Expressly conferred enforceable rights of data subjects

• How?
  • Former Article 29 Working Party: published separate recommendations for BCR applications of controllers and processors, including standard application forms
  • Approval by supervisory authorities
  • Article 47: Detailed conditions for transfers

• Why?
  • Flexibility
  • Low administrative burden post implementation
  • Different versions of BCRs for controllers and processors
International data transfers

Derogations

- Consent
- Performance of contract
- Public interest
- Establishment, exercise or defence of legal claims
- Vital interests
- Transfer from register
- Legitimate interests

Session notes

Derogations (Article 49)

- An exemption from prohibition on transferring personal data outside EEA
- When a country outside EEA does not have adequacy decision and appropriate safeguards are not in place
- Last resort for limited circumstances/specific conditions; strict criteria to be narrowly interpreted

  - Explicit consent from data subject
    - Data subject must understand possible risks to transferring their personal data
  - Where it is necessary for the performance of a contract with the data subject
    - Must be no way to fulfil the contract unless data is transferred
  - Public interest
    - Personal data may be transferred outside EEA for reasons of public interest recognised by EU or member state law only
  - Establishment, exercise or defence of legal claims
    - Designed to cover international litigation scenarios
  - Protection of vital interests of the data subject or other persons
    - Theme that runs through all forms of personal data processing
    - Designed for emergency situations (e.g., if individual must be provided with emergency medical care)
  - Transfer from a register of public information
    - Must comply with any restriction on access to or use of information
    - Must honour conditions imposed by the organisation that compiled the register
  - Legitimate interests of controller
    - Allows international data transfer in wider set of circumstances
    - Transfer must be non-repetitive and concern limited number of individuals
    - Narrow provisions: Protection of individuals’ rights, assessment and documentation, suitable safeguards, notification to data subject and SA of transfer
International data transfers

Restrictions

- Foreign law enforcement requests
- Important reasons of public interest

Session notes

Restrictions

- **Foreign law enforcement requests** (mutual assistance treaty)
  - ‘Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State’ (Article 48)

- **Important reasons of public interest**
  - ‘In the absence of an adequacy decision, Union or Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of personal data to a third country or an international organisation. Member States shall notify such provisions to the Commission’ (Article 49[5])
Session notes

In November of 2020, the European Data Protection Board (EDPB) published step-by-step recommendations for data transfers in the wake of “Schrems II.”

Steps 1 and 2: Map your transfers and verify your transfer mechanism
Know and document what personal data you are transferring, especially if any data belongs to a sensitive category. Verify that the transfer tool your transfer relies on is among those listed under Chapter V of the GDPR (standard contracts, ad hoc contractual clauses, BCRs, consent or GDPR derogation).

Step 3: Assess the sufficiency of non-EEA protections
Is there a law or practice of the third country that may impinge on the effectiveness of appropriate safeguards of the transfer tool? This is where the European Essential Guarantees recommendations become relevant. The EDPB summarizes essential guarantees as:

- Processing based on clear, precise and accessible rules
- Necessity and proportionality need to be demonstrated with regard to legitimate objective pursued
- An independent oversight mechanism should exist
- Effective remedies need to be available to the individual

Resource:
Session notes

Step 4: Identify and adopt supplementary measures

- Identify and adopt supplementary measures that are necessary to bring the level of protection of the data transferred up to EU standard of essential equivalence
- This step is necessary when step 3 reveals that the third-country legislation impinges on the effectiveness of the Article 46 transfer tool. The EDPB provides a list of measures in Annex 2:
  - EDPB outlines additional safeguards and scenarios
  - Technical safeguards include guidance on encryption, pseudonymizations
  - Contractual safeguards - EDPB covers:
    - Transparency
    - Enhanced audits
    - Notification
    - Challenge government access to data in court
    - Contractual agreements to enable data subject rights
  - Organisational measures: internal policies with groups of enterprises, training staff, transparency policies, etc.

Step 5: Take any formal procedural steps the adoption of the supplementary measure may require

- Document approach and seek authorization where required by the chosen transfer mechanism

Step 6: Re-evaluate approach at appropriate intervals to monitor if changes are needed

Resource:
Review question

NOTE: Review questions are intended to help reinforce key topics covered in the module. They are not meant to represent actual certification exam questions.

1. Arrange the options for international data transfers in the order that they should be considered.

A. Appropriate safeguards
B. Adequacy decisions
C. Derogations
Review question

2. Which of the following options for international data transfers is a determination by the European Commission that a third country has achieved an EU-level of personal data protection?

A. Appropriate safeguard
B. Derogation
C. Adequacy decision
3. Which of the following countries have been deemed adequate by the European Commission? Select all that apply.

A. Argentina  
B. New Zealand  
C. Switzerland  
D. Uruguay
Review question

4. Which of the following are appropriate safeguards for international data transfers? Select all that apply.

A. Binding corporate rules
B. Standard contractual clauses
C. Public interest
D. Approved codes of conduct or certification mechanisms
Review question

5. Which appropriate safeguards allow large multinational companies to adopt a policy suite with rules for handling personal data?

A. Ad hoc contractual clauses
B. Reliance on international agreements
C. Standard contractual clauses
D. Binding corporate rules
Review question

6. True or false: Criteria for derogations are strict and should be interpreted narrowly.
Learning objectives

• Discuss the legal bases and data protection considerations for employers processing employees’ personal data
• Determine applicability of EU data protection law and compliance requirements for surveillance, particularly communications data, CCTV, biometric data and location data
• Determine applicability of EU data protection law and compliance requirements for direct marketing, particularly online behavioural advertising
• Determine applicability of EU data protection law and compliance requirements for internet technology and communications, particularly cloud computing, web cookies, search engines, artificial intelligence and social networking services
Session notes

The mix of EU data protection law with local employment law can make compliance in the context of employment complicated.

- **Under Article 88 of the GDPR, member states may by law or collective agreements** provide for more specific rules around processing employees’ personal data; these rules must include suitable and specific measures to safeguard the data subject’s:
  - Human dignity
  - Legitimate interests
  - Fundamental rights
- with particular regard for:
  - Transparency of processing
  - Transfer of personal data within a group of undertakings or a group of enterprises engaged in a joint economic activity
  - Monitoring systems
- **Local employment law** varies considerably across the EU
- **Additionally, an employer may be obligated to communicate with a trade union or works council**
  - In certain jurisdictions, works councils have considerable power over the processing of employees' personal data
  - Compliance may require notifying, consulting with and seeking approval from works councils
Session notes

Under the GDPR, first there must be a lawful basis for collecting and processing personal data. As introduced in Module 4, the legal bases are the grounds employers may rely on to process employee personal data.

- **Fulfilment of an employment contract**: Collecting and using bank account information to process salaries
- **Legal obligation**: Sharing salary information with tax authorities
  - Must be an obligation under EU or member state law
- **Legitimate interests of the employer**: Migrating employee information from one data management system to another
  - Cannot be adverse to employees’ rights and freedoms
  - Cannot be used as grounds for processing special categories of data
  - Cannot be relied on by public authorities
- **Consent?**
  - Difficult to prove because of the unequal distribution of power between the employer and employee
  - Additionally, the processing of employee data may be unlawful or unfair under local law, even if the employee has consented
  - Yet, under some local labour laws, employers are obligated to obtain consent from employees to process their personal data
Session notes
Where sensitive personal data on employees is collected and processed, employers must comply with one of the exceptions specified in Article 9 of the GDPR.

- Consent
  - Not likely legal grounds for processing sensitive employee data
- Establish, exercise or defend legal claims
  - May be necessary, such as an employee’s claim of unfair dismissal
- Carry out obligations and exercise specific rights under employment, social security and social protection law
  - Where authorised by EU or member state law or collective agreement
  - In a number of jurisdictions, employment and labour laws restrict the extent to which sensitive employee data can be processed
  - Local data protection authorities may issue authorisations for specific processing activities
Session notes

Employers process personal data throughout the employment lifecycle for broad reasons; however, records that contain personal data should not be kept longer than necessary.

From the moment an individual applies for a position, the prospective employer begins collecting personal data. After employment has been terminated, an organisation’s legitimate reason to retain an individual’s data diminishes.

Local laws may affect obligations, potentially requiring the employer to retain employee data.
- For example, some health and safety laws require records relating to health and safety checks on individuals who operate machinery to be retained
- If an organisation is obligated to retain personal data on former employees, generally these records should be archived, and internal access should be limited
Session notes

BYOD
- Bring your own device (BYOD) is an issue relevant to every stage in the employment lifecycle
- BYOD poses certain data protection compliance issues since the employer remains responsible as a controller for any personal data processed on the employee’s device for work-related purposes
- BYOD programmes open the door to greater risks to data protection, including data breaches, which could result in substantial penalties and fines under the GDPR

Effective management of BYOD programmes:
- **Provide notice to employees** explaining the consequences of signing up for BYOD and outlining the information the organisation will be able to access (Again, the employer must first have a lawful basis for processing personal data)
- **Implement a BYOD policy** that:
  - Explains to employees how they can use BYOD and their responsibilities
  - Aligns with employment law and the GDPR
  - Protects personal data of individuals, such as employees, customers, patients and sponsors
  - Protects organisational data, such as intellectual property, financial information and trade secrets
  - Enables employee productivity
  - Mitigates network risks
- **Know where the data processed via the device is stored and the measures required to keep the data secure**
- **Ensure the transfer of data from the device to the company’s server is secure** to avoid interceptions
- **Know how to manage data held on the device** once the employee leaves the company or the device is lost or stolen (for example, use of mobile device management software to locate devices and remove data on demand)

Employers must not use background checks to create blacklists, which are generally illegal.
Session notes

Legal requirements
- Member state data protection law and local employment law
- GDPR: Employees’ rights and freedoms balanced against rights of employer; alternatives to monitoring always considered
  - Prevention rather than detection; e.g., blocking websites employer does not want employee to visit

Types of monitoring
- Background checks (e.g., verifying education background)
- Data loss prevention (DLP) technology
  - Tools used to protect IT infrastructure and confidential business information from external and internal threats
  - Inevitably involves processing personal data
- Whistleblowing schemes
  - U.S. Sarbanes-Oxley Act (2002): U.S. companies must have system in place to receive anonymous complaints about potential wrongdoing
  - Conflicting obligations for U.S. companies with EU subsidiaries/affiliates: protect identity of whistle-blower (SOX) versus protect personal data of accused (EU)

To monitor employees lawfully, employer must ensure monitoring is:
- **Necessary**: Can you demonstrate monitoring is really necessary?
- **Legitimate**: Do you have lawful grounds for processing? Is it fair?
- **Proportional**: Is monitoring proportionate to issue?
- **Transparent**: Have employees clearly been informed of monitoring?

Personal data about employees collected through monitoring must be held securely, accessed only by those within the organisation with legitimate reason to view it and deleted when there’s no longer a need to hold onto it (may be business need to retain it).
Session notes
For review purposes
Session notes

Surveillance:
- The observation of an individual or group of individuals
- May be covert or carried out openly, conducted in real time or by access to stored material

Technology-based surveillance examples: Social networks analysis and mapping, data mining and profiling, aerial surveillance, satellite imaging, telecommunications surveillance, CCTV cameras, biometric surveillance, geolocation technologies

Article 23 of the GDPR
- Permits EU or member state law to restrict the rights granted in Chapter 3, ‘Rights of the data subject’
- Must respect ‘the essence of the fundamental rights and freedoms’ and be a ‘necessary and proportionate measure in a democratic society’ (as set out in the Charter and in the European Convention for the Protection of Human Rights and Fundamental Freedoms)
Session notes

Developing technologies continue to break down barriers to surveillance. While public authorities and private-sector entities may have lawful purposes for surveillance, the broadening landscape of available data means broadening scope for invasion of privacy as well.

Public and state agencies for national security or law enforcement purposes

- Must be conducted in a manner to respect individual rights enshrined in the Charter of Fundamental Rights, specifically the right to a private and family life (Article 7) and protection of personal data (Article 8)
- The Law Enforcement Data Protection Directive (LEDP Directive)
  - Recital 66: Although the processing of personal data must be lawful, fair and transparent, this should not prevent law enforcement authorities from carrying out activities (e.g., covert investigations and video surveillance) to:
    - Prevent, investigate, detect and prosecute criminal offences
    - Safeguard against and prevent threats to public security
      - Key requirements: lawfulness, necessity, proportionality and regard for legitimate interests of the natural person
- Laws that fail to appropriately take into account the rights and freedoms of data subjects may be struck down by the CJEU

Private entities

- Surveillance by private entities must be based on legitimate purposes
- In addition to the GDPR, national laws may concern confidentiality, privacy, data protection and other civil rights; e.g., employment law
Session notes

Historically, communication surveillance has involved traditional surveillance activities, such as interception of postal services and human spies; however, surveillance of electronic communications is more prevalent today.

Personal data generated from electronic communications is categorised as either the content of a communication or the metadata.

Content data
- Content of a communication
- Protected by the right to freedom of expression, recognised by laws around the world, including the EU
- Examples: a conversation between parties to a call, words comprising an SMS message, an email subject line, words in the main body of an email, attachments to an email

Metadata
- ‘Data about data’: Information generated or processed as a consequence of a communication’s transmission
- Provides context to content
- Falls within the GDPR’s definition of personal data because it can be used to identify an individual
- Examples
  - Traffic data: Calling and called numbers in relation to a telephone call
  - Location data: Latitude, longitude and altitude of a user’s equipment, direction of travel, level of accuracy of location information, identification of the network cell (Cell ID) in which a user device is located at a certain time, time and location information was recorded
  - Subscriber data: Name of a subscriber, contact details, payment information
Session notes

The ePrivacy Directive’s official title is Directive 2002/58, but it is known by different names, including the Cookie Directive and the Privacy and Electronic Communications Directive.

It sets out rules governing the processing of location, content and traffic data over a public electronic communications network or publicly available communications system—in other words, data passing over public telephone or internet carriers, or services that use a public communications network.

- Location data
  - For collection of individuals’ precise location-based data, opt-in consent is generally required (with the exception of carriers who need the data to provide the service)
- Content data
  - Article 5(1): The confidentiality of the content of communications must be ensured and cannot be intercepted or disclosed to third parties unless there is consent from all users
  - Article 15(1): Member states can introduce some exemptions if necessary for very limited purposes
- Traffic data
  - Access to traffic data is limited
  - Telecommunications carriers can process traffic data for the purpose of conveying communications and possibly for some limited marketing activities with the user’s consent
- Private networks (e.g., a corporate intranet)
  - ePrivacy rules do not apply
  - Monitoring considerations, as discussed earlier in this module, are still relevant
- Provision allowing for the interception of a communication when an organisation has a lawful business purpose for accessing data going through their public networks
  - Member states, under their individual laws, may pass legislation defining lawful business purposes
Session notes

Closed circuit television—and other modes of video surveillance (CCTV)

- **Lawfulness of processing**: Prior to carrying out surveillance, the controller should determine the lawfulness of processing (consent likely not possible), including for biometric data (Article 9)
  - A controller may need to rely on a provision in member state law to conduct video surveillance in a particular context
  - A decision to use CCTV should be made only if other, less-intrusive solutions that do not require image acquisition have been considered and found to be clearly inapplicable or inadequate for the intended lawful purpose (A DPIA should document these investigations and inadequacies)

- **Data protection impact assessment**: A DPIA is required in some circumstances—if the video surveillance is considered to be high risk, if it involves the systematic monitoring of a publicly accessible area on a large scale, or if video surveillance has been included by the relevant supervisory authority on a list of data processing operations that require a DPIA

- **Prior checking**: In many countries, using CCTV triggers the requirement to notify the local regulator and, in some circumstances, seek authorisation

- **Proportionality**: The particular system and technology used for surveillance should be proportional to the purpose (e.g., Remote control, zooming functionality, facial-recognition, and sound-recording may not be necessary)
  - Key aspects of the CCTV and processing of its footage must be proportionate to the purpose, such as the visual angle so that monitoring of irrelevant spaces is minimised

- **Information provision**: For overt video surveillance, controllers must comply with the transparency requirement of the GDPR where the controller may not have a direct relationship with the affected data subjects (e.g., camera covering large, public space)
  - As the information that may be made available via a sign is unlikely to contain all the details prescribed by Articles 13 and 14 of the GDPR, the controller should be prepared to provide the full information necessary when a data subject makes contact

- **Individual rights**: Under the GDPR, data subjects have rights related to the processing of their personal data (e.g., right to access, yet may pose the challenge of protecting others’ privacy)

- **Measures to protect the personal data and rights of individuals**: These may include staff training, a CCTV policy, and regular reviews to ensure compliance
Session notes

Location-based services (LBS) utilise information about location to deliver a wide array of applications and services.

LBS may be derived from satellite network-generated data, such as GPS; cell-based, mobile network-generated data; and chip-card generated data.

Location data is referred to as an identifier in the GDPR’s definition of personal data. If location data can be used alone or in combination with other information to identify someone, then it should be considered personal data.

Google has identified three main areas of location data that it uses to deliver its services:

- Implicit location information, such as search terms
- Internet traffic information, such as IP addresses
- Device-based location services, such as Google Maps
Session notes

Biometrics data defined in Article 4(14) of the GDPR as ‘personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data’.

Main uses of biometrics systems:

Identification: Who are you? (i.e., photographs loaded up to social media; identification of individuals through facial recognition)
Authentication: Are you who you claim to be? (i.e., fingerprint to authenticate identity when accessing a mobile device, computer; palm print to access a secure building)

Article 9: For biometric data to be included as a special category, the purpose for processing must be for uniquely identifying a natural person
Session notes

What is direct marketing?

- Former Article 29 Working Party: To fall under the scope of direct marketing, a communication, by whatever means of any advertising or marketing material, should be directed to particular individuals.
- Messages that do not process personal data to communicate the marketing message or those that are purely service-related in nature are not direct marketing.
Chat: Let’s talk about...
Why is direct marketing one of the most complex areas of data protection law?
Session notes

Direct marketing is regulated both by the GDPR and the ePrivacy Directive (discussed on the following slide). The GDPR:

- Applies to all direct marketing communications, regardless of channel
- Applies to online advertising targeted at individuals based on their internet browsing history
- Provides individuals an absolute right to object to any form of direct marketing at any time
  - Extends to processing based on legitimate interest
- Requires controllers to:
  - Explicitly and clearly inform individuals of their right to opt out at the time of the first communication with them
  - Allow individuals to opt out across all marketing channels
  - Honour opt-out requests in a timely fashion and at no cost to the individual
  - Remove personal data and profiling after an individual has opted out (unless retention of personal data is strictly required)
    - Controllers should suppress rather than delete contact details because they do not want to risk reacquiring that individual’s details later and beginning marketing to them again
  - Ensure all compliance requirements under the GDPR are met

Some member states require controllers to cleanse their contact lists against applicable national opt-out registers before sending direct marketing.
Session notes

In addition to the GDPR, direct marketing is regulated by the ePrivacy Directive, which applies to ‘digital’ marketing communications—direct marketing communicated over electronic communications networks, such as by phone, fax, email and SMS or MMS. The ePrivacy Directive:

- Specifies rules that impact the use of online behavioural advertising
- Differs in interpretation and enforcement across member states (e.g., B2B marketing)
- Requires that specific information is provided to recipients (e.g., a valid address to which they can send an opt-out request that is appropriate to the medium of the marketing communication)

- **Postal marketing** is not subject to the ePrivacy Directive
- **Telephone marketing** (telemarketing) is subject to the ePrivacy Directive
  - Article 13(3): Member states decide whether person-to-person telemarketing should be conducted on an opt-in or opt-out basis
    - Individuals must have a means to opt out for free
    - Most member states have implemented national opt-out registers, which typically must be checked against the controller’s call lists
  - Consent is required for marketing through automated calling systems
- **Electronic mail marketing** is subject to the ePrivacy Directive
  - Electronic mail marketing: Email and SMS/MMS
  - In general, prior consent is required
  - Limited exemption from the strict opt-in requirement for direct marketing by electronic mail to individuals whose details the data controller obtained ‘in the context of the sale of a product or service’ is allowed
    - The controller must market its own similar products and services
    - Individuals must have the ability to opt out at the time their contact details are collected
    - Individuals must be reminded of their ability to opt out in each subsequent marketing communication
Session notes
For review purposes
Session notes

**GDPR**
- Recital 30: Where the information collected from cookies is personal data, its collection and analysis amount to processing subject to the GDPR
- Who is a controller?
  - The website operator is a controller of the personal data gathered by its own first party cookies
  - Where the third party determines the means and purposes of processing of the personal data gathered from its third-party cookies, it is a controller
- Many organisations now rely on consent to process personal data in the form of online identifiers
  - Article 4: Consent is any ‘freely given, specific, informed and unambiguous indication of a data subject’s wishes’
  - Article 7: Consent must be presented separate from other matters in ‘an intelligible and easily accessible form, using clear and plain language’

**ePrivacy Directive**
- Article 5(3): Under member state law, organisations must obtain prior informed consent for storage or access to information stored on a user’s terminal equipment
- ‘Strictly necessary’ cookies and those used solely for carrying out communication transmission are exempt from the consent requirement
- Prior to the GDPR, valid consent under the ePrivacy Directive—as implemented in member state laws—was widely interpreted to be met with a visible pop-up notice announcing the use of cookies, followed by the user’s continued use of the site. Given the GDPR’s requirement of ‘specific, informed, and unambiguous indication’ of consent, many organisations now are requiring users to affirmatively interact with the cookie banner, if not also use a consent tool. The CJEU recently clarified cookie consent requirements in that consent: must be obtained through active behavior; applies to processing and storing non-personal data information; include information regarding cookie duration and access by third parties

In addition to provisions under EU law, best practices around the use of cookies include storing only encrypted personal data, providing notice, using persistent cookies only if justified by the need, and setting reasonable expiration dates for cookies.
OBA is website advertising targeted at individuals based on the observation of their behaviour over time.

OBA increasingly happens through third-party advertising networks.
- Third-party advertising networks have relationships with partnering website publishers that enable it to place cookies on individuals’ computers with unique identifiers
- As websites track individuals’ website activities, profiles are assigned to unique identifiers, enabling ad networks to deliver advertising based on individuals’ interests

GDPR
- Clearly identifies information collected for OBA purposes as personal data; its definition of personal data specifically provides ‘online identifier’ as an example
- According to the former Article 29 Working Party, all parties to a third-party ad network relationship potentially may attract compliance responsibilities under the GDPR (the ad network itself, which will often qualify as a controller; a website publisher, which may qualify as a joint controller; and advertisers, which may qualify as independent controllers)

ePrivacy Directive
- Will generally apply to OBA regardless of whether or not OBA information collected from individuals constitutes personal data
- Article 5(3) (amended, 2009): The use of cookies to store or access information in an individual’s computer is allowed only on the condition that the individual concerned has given their consent, having been provided with clear and comprehensive information
Session notes

Because a controller has significantly more obligations under the GDPR, distinguishing between the controller and processor in a customer-cloud services supplier relationship is essential. This distinction may not always be clear.

A cloud services supplier may determine technical and organisational means of processing (for example, hardware) and remain a processor.

Even if the cloud provider is not directly subject to the GDPR, the cloud provider’s customer may be subject to it, in which case the data processing contract should contain required controls and obligations as set out in the GDPR.

The EU does not have specific legislation regarding cloud computing; however, the technology-neutral GDPR, where applicable, sets out controller and processor obligations. Determining whether the GDPR applies to cloud computing services, as according to Article 3 of the GDPR, may pose challenging for cloud service providers. As covered in Module 4, Article 3 applies where either:

- The processing relates to the activities of an EU establishment of the controller
- Or the processing relates to offering goods or services to individuals in the EU, or to monitoring their behaviour, even when the controller or processor is not established in the EU
Session notes

Search engines are services that find information on the internet. They process large volumes of data, routinely including user IP addresses, cookies, user log files and third-party web pages.

Who is a controller of personal data processed by search engines?

- **Search engines**: Because search engines determine the purposes and means of processing data about their users, they are controllers of that personal data
  - *Google v. AEPD*
    - In 2014, the CJEU ruled on the Google v. AEPD case, which required that Google remove from its search results links to a 1998 newspaper article about the plaintiff’s foreclosed house
    - This established that search engines are also controllers of the personal data contained in third-party web pages
    - Because of the Google v. AEPD decision, search engines outside the EU are also likely subject to the GDPR in respect of their processing of personal data contained in third-party web pages if they have an EU establishment whose activities are economically linked to the search engine’s core activities

- **Search engine marketers**: When web traffic data is processed by search engines and provided as analytics, such as Google Analytics, to search engine marketers that fall within the scope of the GDPR, the organisations conducting the search engine marketing are also controllers
  - Search engine marketers can take certain steps to ensure that aspects of the web traffic analysis process are anonymised (e.g., ensuring that data, including IP addresses, is not stored in Google Analytics even after the user has accepted the placement of cookies; anonymising IP addresses before storage or processing takes place)
Social networking services (SNS) create opportunities for various parties and individuals to collect and use personal data. As a result, there may be multiple controllers.

**Who is a controller?**
- Social networking services because they provide platforms for publishing and exchanging personal information, as well as determine the use of personal information for advertising purposes
- Authors of applications designed for SNS platforms that provide services in addition to the SNS
- Users who act on behalf of an organisation
- User knowingly extend access to personal data beyond selected contacts

**Sensitive, third-party and children’s personal data**
- Sensitive personal data: Explicit consent usually is required to publish personal data on the internet, unless it is published by the data subject. An SNS requesting personal data (for example, for an individual’s profile) must ensure the individual knows that provision of the data is voluntary.
- Third-party personal data: If third-party individuals’ personal data is published (for example, photo tags), the SNS must have a legal basis for processing that personal data. According to the former Article 29 Working Party, third-party data of individuals who are not members of the SNS may not be aggregated to form profiles of those individuals.
- Children’s data: As discussed in Module 4, processing children’s data on the basis of consent requires parental consent. This applies to children under 16 years old; member States may lower this age limit to 13 years old. Processing on the grounds of legitimate interest may not be possible (GDPR, Article 6[f]). According to the former Article 29 Working party, a controller should have regard for the best interests of the child.
Let’s talk about...
How can an SNS be transparent about its processing of personal data?

Chat: Let’s talk about...
How can an SNS be transparent about its processing of personal data?
Session notes

Artificial intelligence is the simulation of human intelligence created by machines and computers. With the ability to learn, reason and evaluate, AI can replace humans and act on their own to make automated decisions. Machine learning, which is a type of AI, is driven by available data. The machine learns to identify patterns in the data and applies that to new data. This enables better understanding of human behaviors and activities.

Provisions within the GDPR affect the AI functions of automated decision-making. Article 22, discussed in Module 5, highlights data subject rights in connection with profiling and automated decision-making.

Organisations implementing AI technology will want to ensure privacy regulations are being met in conjunction with the technology.

The EU initiative on AI includes:

- Boosting the technological and industrial capacity and AI uptake across the public and private sectors
- Preparing for socio-economic changes as AI modernises education, training, labour markets and social protection systems
- Focusing on high-risk uses of AI
- Restricting certain practices, such as use of facial recognition in publicly accessible places for law enforcement
- Guaranteeing human oversight of AI systems
- Ensuring ethical principles
  - Respect for human autonomy, prevention of harm, fairness and explicability

Resources:

European Commission: Strategy for Artificial Intelligence

Ethic guidelines for Trustworthy AI
https://iapp.org/media/pdf/resource_center/AIEthicsGuidelinespdf.pdf
Review question

NOTE: Review questions are intended to help reinforce key topics covered in the module. They are not meant to represent actual certification exam questions.

1. Which types of laws should be considered when processing employees’ personal data? Select all that apply.

   A. Local employment law
   B. EU data protection law
   C. Member state data protection law
Review question

2. Under the GDPR, which legal basis for processing personal data would be difficult to use for processing employee data?

A. Fulfilment of an employee contract
B. Legal obligation
C. Legitimate interests of the employer
D. Consent
Review question

3. True or false: Some employers may be required to consult with works councils and/or trade unions to process employees’ personal data.
4. True or false: BYOD policies are designed to protect employees’ personal data only.
Review question

5. True or false: Alternatives to employee monitoring should always be considered first.
Review question

6. The ePrivacy Directive governs the processing of which types of data? Select all that apply.

A. Location data
B. Content data
C. Traffic data
7. True or false: The ePrivacy Directive governs the processing of data through both private and public carriers and communications networks.
8. True or false: Under the GDPR, individuals have the absolute right to object to any form of direct marketing at any time.
9. Which forms of marketing are subject to the ePrivacy Directive? Select all that apply.

A. Postal marketing
B. Telephone marketing
C. Electronic mail marketing
Review question

10. Which of the following parties involved in online behavioural advertising may qualify as a data controller? Select all that apply.

A. An ad network
B. A website publisher
C. An advertiser
Module 9: Security of processing

Learning objectives

• Summarise the considerations and duties of controllers and processors for ensuring the security of personal data
• Describe four major attributes of secure processing systems and services
• Describe requirements and best practices for ensuring security of personal data
• Outline the requirements related to informing the supervisory authority (SA) and data subjects of a data breach
You can have security without data protection, but you cannot have data protection without security.

Session notes
You can have security without data protection, but you cannot have data protection without security.

- The majority of data protection enforcement in Europe is related to security incidents
- Data protection and security are related but not the same
- Security supports compliance with GDPR in many ways
Session notes

Attributes of security controls (Article 32[1][b])

- ‘CIA’ should be well-known to InfoSec professionals, but perhaps new to others
- **Confidentiality**: Individuals, entities, systems or applications access data on a need-to-know basis
- **Integrity**: Controls are in place to ensure data is accurate and complete
- **Availability**: Data is accessible when needed for a business activity
- **Resilience**
  - New attribute in GDPR
  - Data is able to withstand and recover from threats
Chat: Knowledge check

Gina is working from home today. She is trying to access client data she needs from her organisation’s remote connection; however, she cannot remember her access password. She emails her coworker in the IT department for help. They provide her with a link that will allow her to reset her password. After answering a security question correctly, Gina resets her password and accesses the secure client data she needs.

Which of the four security attributes does this scenario exemplify?

- Confidentiality
- Integrity
- Availability
- Resilience
What does the GDPR say about security? (Article 32)

- The controller and the processor shall provide...
  - Appropriate technical and organisational measures
  - What is appropriate security?
  - The law does not specify
  - The law does not require absolute security (a breach may still be possible)

- To ensure...
  - A level of security appropriate to the risk
  - Risks may include accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to personal data
  - Risk-based approach requires a risk assessment
  - Risk assessment determines controls

- Taking into account...
  - State of the art: Security controls should be chosen based on a consensus of professional opinions
  - Costs of implementation: Controls should reflect good management decisions
  - Nature (e.g., special categories)
  - Context in which processing is taking place (e.g., investigating an employee suspected of wrongdoing)
  - Scope (i.e., how much data)
  - Purpose of processing
  - In addition, the entire information life cycle should be considered, including potential security threats and harm that may come to personal data

- Certification mechanisms and codes of conduct may be used to demonstrate compliance
  - These must be approved by supervisory authorities
**Protection mechanisms**

The technology stack
- Encryption, antivirus and antispam technology, firewalls, identity and access management, incident detection, data loss prevention, two-factor authentication, IP log management, regular security code peer review

The physical environment
- Sophisticated entry control systems, closed-circuit television (CCTV), lock-and-key and clean-desk policies

---

**Session notes**

- **The technology stack**
  - Electronic information main focus of data protection law
  - Security-enhancing technologies: encryption, antivirus and antispam technologies, firewalls, identity and access management, incident detection, data loss prevention, two-factor authentication, IP log management, regular security code peer review
  - A key focus of security technologies: filtering electronic communications and monitoring use of IT and communication systems
    - Often involves complex privacy and employment law issues (see Module 8)
  - Testing the ability of the technology stack to withstand cyberattacks and misuse
    - Penetration (pen) testing by ‘ethical hackers’ and testing coding security

- **The physical environment**
  - Sophisticated entry control systems, closed-circuit television (CCTV), lock-and-key and clean-desk policies
  - Subject to same restrictions as other monitoring controls
Security of processing

Article 28: The controller-processor relationship

- Article 28(1): flow down security principle and requirements to the processor
- Processors must be limited to those who can provide ‘sufficient guarantees’ about the implementation of appropriate technical and organisational measures for compliance with the Regulation and for the protection of the rights of data subjects
  - ‘Sufficient guarantees’: Much more than contracts
  - Assurance mechanisms: Appropriate checking and vetting of the processor by the supplier via a third-party assessment of certification validations, before and after creating a contract

Session notes

See also Module 3.
Session notes

Data breach notifications

- Article 4(12): Personal data breach definition
  - Accidental or unlawful
  - Breach of security leading to: accidental or unlawful destruction, loss, alteration, unauthorised disclosure and access
  - Personal data transmitted, stored and otherwise processed

- **Processor** notification duty
  - Article 33(2): Notification to **controller**
    - Without ‘undue delay’
    - Timed from becoming ‘aware’ of breach

- **Controller** notification duties
  - Article 33(1): Notification to **SA**
    - Without ‘undue delay’ and within 72 hours after becoming aware of the breach
      - When does a controller become aware of a breach? ‘When that controller has a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised’ (Former Article 29 Working Party)
    - Delay permitted if ‘reasoned justification’
    - Exempt if unlikely to result in a risk to the rights and freedoms of natural persons

- Article 34: Notification to **data subject**
  - Applies if ‘high risk’
  - Without ‘undue delay’
  - Exemptions for: ‘Unintelligible data’, high risk negated by measures taken and disproportionate effort = public communication
  - Regardless of controller’s decision, SA may decide data subject shall be notified
Session notes

Data breach notifications

- **Controller to SA**
  - **Who?**
    - Categories of data subjects
  - **How many?**
    - Approximate number of data subjects and data records
  - **What types?**
    - Categories of data records
  - **Contact**
    - Name and contact details of data protection officer (or other contact point if additional information can be obtained)
  - **Description of likely consequences**
  - **Follow-up**
    - Measures taken or to be taken

- **Controller to data subject**
  - Clear and plain language
Security of processing

Notification rules in summary

<table>
<thead>
<tr>
<th>Notification to controllers (Article 33[2])</th>
<th>Notification to supervisory authority (Article 33 [1])</th>
<th>Notification to data subjects (Article 34)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Sole notification duty for processors</td>
<td>• Without 'undue delay' and within 72 hours</td>
<td>• Applies if 'high risk'</td>
</tr>
<tr>
<td>• Without 'undue' delay</td>
<td>• Delay permitted if 'reasoned justification'</td>
<td>• Without 'undue delay'</td>
</tr>
<tr>
<td>• Timed from becoming 'aware' of breach</td>
<td>• Exempt if 'unlikely' to result in risk</td>
<td>• Exemptions for:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• (a) 'unintelligible data'</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• (b) high risk negated by measures taken</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• (c) disproportionate effort = public notice</td>
</tr>
</tbody>
</table>

Personal 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” (Article 4[12])

Session notes

For review purposes
Chat: Your outlook

Under what circumstances would a data breach result in a high risk to the rights and freedoms of individuals?

Follow-up chat

When would a breach not pose a high risk?
Session notes

NIS Directive

- Effective 9 May 2018
- First cybersecurity law to cover entire EU
- While not specifically concerned with personal data, will indirectly bolster its security within organisations regulated by the Directive
- Three focuses
  - National capabilities: Compel development of national cybersecurity strategies and structures by EU member states
    - National Computer Security Incident Response Teams (CSIRTs)
    - Cybersecurity regulators
    - Operators of ‘essential services’
  - Cross-border collaboration: Enhance cooperation between the member states
    - Cooperation Group to coordinate CSIRTs and develop best practices
  - National supervision of critical sectors: Improve security levels of operators of essential services (energy, water, transport, health and banking sectors) and digital service providers (online marketplaces, online search engines and cloud computing services)
    - Member state laws that set out security requirements and incident notification requirements for these entities
Session notes

German state DPA issues country's first GDPR fine (2018)

The data protection authority of Baden-Württemberg administered the first fine in Germany for violations of GDPR, according to a blog post from Hogan Lovells’ Chronicle of Data Protection. The DPA fined an unnamed social media provider 20,000 euros after it suffered a data breach. The social media company informed affected users of the breach and the agency of its security failings. The DPA decided to penalise the company after the agency discovered it stored passwords in plain text, a violation of Article 32 of the GDPR.
France's data protection authority, the CNIL, fined the real estate company Sergic 400,000 euros for violations of the GDPR. A complaint received by the CNIL alleged users could access documents from other individuals on the site by modifying a URL. The documents contained individuals' identity cards, tax notices, account statements and other information. An investigation conducted by the DPA found Sergic was aware of the vulnerability since March 2018. The DPA discovered Sergic did not implement any form of user authentication for those who could access the documents, which factored into the decision to penalise the company.
Review question

NOTE: Review questions are intended to help reinforce key topics covered in the module. They are not meant to represent actual certification exam questions.

1. CIAR stands for _____.

   A. Continuity, information, access, risk assessment
   B. Confidentiality, information, availability, risk assessment
   C. Confidentiality, integrity, availability, resilience
   D. Continuity, integrity, access, resilience
Review question

2. True or false: A processor is responsible for implementing appropriate technical and organisational measures to keep personal data secure.
3. A controller must notify the SA of a personal data breach if _____.

A. The breach is likely to result in a risk for the rights and freedoms of natural persons.
B. The breach is likely to result in a high risk for the rights and freedoms of natural persons.
Module 10: Accountability

Learning objectives

• Recognise accountability implications of the GDPR’s Article 24 for controllers and processors
• Outline steps for designing a data protection programme, including a data protection impact assessment and data protection policy
• Summarise record-keeping requirements of controllers and processors
• Describe the protections, tasks and responsibilities of data protection officers
Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary. (Article 24[1])

Session notes

Accountability: The ability to demonstrate that a data protection programme has been implemented and run in compliance with the law.

Article 24(1)

- Nature, scope, context and purposes ... as well as risks
  - Risk-based approach
- Appropriate technical and organisational measures
  - All technical and non-technical measures
- Demonstrate
  - Records of controllers and processors available to SA
- Reviewed and updated
  - Continuous improvement and communication
  - Testing and auditing
- In practice: data protection programme
  - Data protection by design/by default
  - Data protection impact assessments (DPIAs)
  - Maintaining data processing records
  - Appointing data protection officer (DPO)

Auditing privacy programs

- DPAs have the ability to carry out audits and inspections of premises and processing equipment
  - Data protection written systems
  - Data protection business operations
- DPAs can issue warnings to stop business activities if data processing practices are suspicious
- Regulators have the right to conduct audits
Chat: Share your experience

What is data protection by design?
Session notes

Implementation of technical and organisational measures should take place ‘both at the time of the determination of the means for processing and at the time of the processing itself’ (Article 25).

Data protection by design

- **Data protection built into product life cycles**, rather than as afterthought
- Integrate necessary **safeguards** into the system
  - GDPR examples: **Data minimisation, pseudonymisation**
- **Assess/mitigate product risks** to meet data protection by design requirements
Session notes

Data protection by default

- Where a product/service provides users with multiple setting options, the most data protective settings are default
  - Users have to opt-in to any setting that presents greater risks
- By default, the product/service processes only necessary personal data
  - Considerations: purpose, amount of personal data collected, extent of processing and storage period
- Limited accessibility to personal data

For practical examples of privacy by default, refer to Piotr Foitzik's IAPP The Privacy Advisor article, ‘Privacy by default in online services’: https://iapp.org/news/a/privacy-by-default-in-online-services
Session notes

Data protection impact assessment (DPIA)
- To help incorporate data protection considerations into organisational planning
- To help demonstrate compliance to supervisory authorities
- Article 35: Considerations
  - Nature, scope, context, purpose, type of processing
  - Use of new technologies
- Article 35: Conditions
  - High risk to rights and freedoms of data subject
    - Examples: systematic, extensive evaluation of personal aspects based on profiling or processing of special categories
    - Large-scale processing of special categories
    - Monitoring public areas systematically and on large scale
    - GDPR, Article 29 Working Party Guidelines on DPIAs and member state lists
  - SA may set out other specific processing operations that qualify as high risk
- Article 35: Contents of DPIA
  - Description of processing
  - Assessment of necessity, proportionality and risks to rights and freedoms of data subject
  - Measures (controls) to address risks
- Article 36: Prior consultation with SA
  - Prior to processing when DPIA indicates high risk to data subject
  - Contents: DPIA, responsibilities of controllers and processors, purposes and means of processing, measures and safeguards, and contact details of DPO
  - If SA thinks processing will not be compliant or controller has not sufficiently mitigated risks
    - Will provide advice to controller
    - Can block processing activities within eight weeks (six additional in complex situations)
Session notes

Data protection policy used ‘where proportionate in relation to processing activities’ (Article 24[2]).

- Amongst other measures
- As part of larger data protection programme
- GDPR does not specify required contents

Good practices for design:

- **Language**
  - Use language that speaks to the recipients
- **Contents**
  - Communicate to the recipients what to do, what not to do and consequences
  - Use principles concretely (e.g., to explain a specific example)
- **Goals**
  - Consider how metrics may be used to demonstrate results
  - Ensure tasks are achievable, realistic, relevant and timely (e.g., do not refer to outdated technologies)
Chat: Brainstorm
Topics that may be covered in a data protection policy

Follow-up chat
What types of metrics may be used to demonstrate results?
Session notes

- SA may request copy of processing records from controller, processor and representatives
- Recording obligation triggers for controllers and processors: Processing that ...
  - Organisations of 250 or more employees
  - Is likely to result in risk to rights and freedoms of data subject
  - Is not occasional
  - Includes special categories of data or data relating to criminal convictions/offences

Controller records (Article 30)

- Name and contact information of controller, representatives and DPO
- Categories of data subjects
- Categories of personal data
- Recipients
- International data transfers and appropriate safeguards
- Time limits for erasure
- Technical and organisational security measures
Session notes

**Processor records** (Article 30)
- Name and contact information of processor, controller, representatives and DPO
- Categories of processing
- International data transfers and appropriate safeguards
- Technical and organisational security measures

Good practice: Keep a log of all processing activities to show competence/compliance of controllers, processors and representatives in the event of an incident.

**International data transfers:**
Additions of codes of conduct and certification mechanisms as adequacy mechanisms. EDPB issued guidance to help clarify procedures and rules regarding codes of conduct as well as on the accreditation of certification bodies under Article 43.
Session notes

Role of the data protection officer (DPO) (Article 37)
- Formerly Personal Data Protection Official under the Directive
- Staff member or contractor
  - Appointed by controller or processor
  - Tasked with ensuring and demonstrating compliance with data protection law
- Expert in data protection law and practices
- Legally required position (under some circumstances)
  - Core activities of controller or processor include:
    - Processing activities that require ‘regular and systematic monitoring’ of data subjects on ‘large scale’
    - Processing sensitive data (or personal data relating to criminal convictions/offences) on a ‘large scale’
    - Processing by public bodies, other than courts acting in judicial capacity
- Union or member state law
- DPO appointed voluntarily
  - Still subject to GDPR requirements
Let’s talk about...

How does the Article 29 Working Party further define core activities, large-scale, and regular and systematic monitoring?

Chat: Let’s talk about...

How does the Article 29 Working Party further define core activities, large-scale, and regular and systematic monitoring?
Session notes

DPO tasks and responsibilities (Articles 38-39)

- **Monitor compliance**
  - ‘Collect information to identify processing activities’
  - ‘Analyse and check the compliance of processing activities’
  - ‘Inform, advise and issue recommendations to the controller or the processor’
  - Manage internal data protection activities, train staff and conduct internal audits

- **Advise controller and processors**
  - Including DPIAs (whether or not to conduct one, methodology, in-house versus outsourced, safeguards, correct implementation and analysis of results in regards to compliance)

- **Manage risk**
- Cooperate with SA
- Communicate with data subjects and SA
- Exercise professional secrecy
Session notes

Controller and processors ensure...

- Communication with/involvement of DPO in all issues related to personal data protection
- Access to personal data and processing operations
- Resources to help DPO carry out tasks
  - ‘Active support’ from senior management
  - ‘Sufficient time for DPOs to fulfil their duties’
  - ‘Financial resources, infrastructure ... and staff’
  - Communicating the DPO designation ‘to all staff’
  - ‘Access to other services within the organisation’
  - ‘Continuous training’
- Safeguards to enable DPO to perform tasks independently
  - ‘No instructions by the controllers or the processors regarding ... the DPO’s tasks’
  - ‘No dismissal or penalty ... for the performance of the DPO’s tasks’
  - ‘No conflict of interest with possible other tasks and duties’
    - ‘The DPO cannot hold a position within the organisation that leads them to determine the purposes and the means of the processing of personal data’
- DPO reports to highest levels of management
Accountability

Summary of responsibilities

<table>
<thead>
<tr>
<th>Accountability requirement</th>
<th>Controllers</th>
<th>Processors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data protection by design</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Data protection by default</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Data protection impact assessments</td>
<td>Yes (where required)</td>
<td>No (but duty to assist Article 28 terms)</td>
</tr>
<tr>
<td>Data protection officer</td>
<td>Yes (where required)</td>
<td>Yes (where required)</td>
</tr>
<tr>
<td>Record-keeping</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Security</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Data breach reporting</td>
<td>Yes (to SAs and data subjects)</td>
<td>Yes (to controller)</td>
</tr>
</tbody>
</table>
Session notes

Article 27

- Article 3(2) processing:
  - Of data subjects in the EU by a controller or processor not established in the EU
  - In relation to offering goods or services or monitoring behaviour
- Exceptions for processing:
  - Occasional, does not include, on a large scale, processing of special categories of data or processing of personal data relating to criminal convictions
  - And unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing
- A representative should be established in member states of those data subjects
- The representative must be mandated by the controller or processor to be addressed in addition to or instead of the controller or processor
  - In particular by supervisory authorities and data subjects
- The designation of a representative must be made without prejudice to legal actions
  - Could be initiated against the controller or processor
Review question

NOTE: Review questions are intended to help reinforce key topics covered in the module. They are not meant to represent actual certification exam questions.

1. True or false: Both controllers and processors have accountability obligations under the GDPR.
Review question

2. True or false: Data protection by design begins before processing and incorporates data protection considerations into the planning phase.
Review question

3. What are the main values of a data protection impact assessment (DPIA)? Select all that apply.

A. Incorporating data protection considerations into organisational planning
B. Determining the purpose of processing personal data
C. Demonstrating compliance to supervisory authorities
4. True or false: The GDPR requires controllers to always contact the SA following a DPIA and before processing personal data.
5. True or false: The GDPR requires a data protection policy to be used ‘where proportionate in relation to processing activities’.

Review question

5. True or false: The GDPR requires a data protection policy to be used ‘where proportionate in relation to processing activities’.

Module 10: Accountability
Review question

6. Which of the following must be included in controllers’ personal data processing records but not in processors’ records?

A. Purposes of processing
B. International data transfers being made and the measures put in place to ensure they are lawful
C. A general description of technical and organisational security measures that have been implemented
Review question

7. True or false: The data protection officer must be an expert in data protection law and practices.
8. Which of the following are circumstances that require an organisation to appoint a DPO? Select all that apply.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>A.</td>
<td>The controller is a public authority.</td>
</tr>
<tr>
<td>B.</td>
<td>The core activities of the controller or processor include regular and systematic monitoring of data subjects on a large scale.</td>
</tr>
<tr>
<td>C.</td>
<td>The core activities of the controller or processor consist of large-scale processing of special categories of data.</td>
</tr>
</tbody>
</table>

Review question

8. Which of the following are circumstances that require an organisation to appoint a DPO? Select all that apply.

   A. The controller is a public authority.
   B. The core activities of the controller or processor include regular and systematic monitoring of data subjects on a large scale.
   C. The core activities of the controller or processor consist of large-scale processing of special categories of data.
Learning objectives

• Describe the role, powers and procedures of the supervisory authorities
• Describe the composition and tasks of the European Data Protection Board
• Describe the role of the European Data Protection Supervisor
• Summarise the remedies against, liabilities of, and potential penalties for controllers and processors, particularly administrative fines
Supervision and enforcement
The SA role

- Promote, monitor and enforce GDPR application
- Promote awareness
- Conduct investigations
- Protect fundamental human rights

Session notes
The SA role (Articles 51-57)
- Also known as data protection authority (DPA)
- Promote, monitor and enforce GDPR
- Promote awareness
  - Help organisations understand their obligations under GDPR
  - Serve in advisory capacity so organisations may approach them for advice on data protection issues
- Conduct investigations on GDPR compliance
- Protect fundamental human rights, including...
  - Raise public awareness
  - Provide information to individuals upon request
  - Manage data subject complaints
- Draw up annual reports that explain...
  - Data protection in their country
  - Current issues
  - Agenda for following year
- Facilitate free flow of personal data within EU
  - Support fundamental role of EU to promote free trade and free movement of data
Knowledge quest
What powers do supervisory authorities have over controllers and processors?

## Chat: Knowledge quest
What powers do supervisory authorities have over controllers and processors?

<table>
<thead>
<tr>
<th>Investigative</th>
<th>Corrective</th>
<th>Authorisation and advisory</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Order the controller/processor to provide information required for performance of its tasks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Conduct data protection audits</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Review certifications</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Notify controllers/processors of alleged GDPR infringements</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Obtain from controller/processor access to personal data necessary for performance of its tasks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Obtain access to premises</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Issue warnings</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Issue reprimands</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Order compliance with data subject request</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Order notification to data subject of breach</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Order controller/processor to bring processing operations into compliance</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Order communication to data subject of data breach</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Ban processing (temporary or definitive)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Order rectification, restriction or erasure of data</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Suspend international data transfers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Withdraw certifications</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Impose administrative fines</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Suspend international data flows</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Provide advice (prior consultation procedure)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Issue opinions to institutions, bodies, public</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Authorise processing of personal data (if required)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Issue opinion/approve draft codes of conduct</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Approve certification criteria</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Accredit certification bodies</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Issue certifications and approve criteria</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Adopt standard data protection clauses</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Authorise contractual clauses</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Authorise administrative arrangements between public authorities/bodies for appropriate safeguards related to transfers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Approve BCRs</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Supervision and enforcement
SA powers continued

• Subject to appropriate safeguards
• Member state law

Session notes
SA powers continued (Article 58)
• Subject to appropriate safeguards, including effective judicial remedy and due process
• Member state law
  • Provides SA with power to bring GDPR infringements to judicial authorities
  • May also provide for additional SA powers
Session notes

Before identifying the lead supervisory authority for cross-border processing, the controller/processor must determine if cross-border processing is taking place.

The criteria for identifying the lead SA for an organisation with more than one establishment in the EU makes it possible for a company to have several lead SAs—if it conducts several cross-border activities whose related decisions take place in more than one location.

- Lead supervisory authority: primary regulator responsible for cross-border processing activities of a controller/processor and coordinating operations of all SAs concerned
- Cross-border processing
  - ‘Processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State.’
  - Or, ‘processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State’ Article 4(23). Article 29 Working Party: ‘Supervisory Authorities will interpret “substantially affects” on a case by case basis.’
- If cross-border processing, identify the lead SA
  - Single establishment in the EU = SA of the place of establishment.
  - More than one establishment in the EU = SA of the place of central administration—unless decisions about purposes, means and implementation of processing take place at a different location. If so, the lead is the SA of that location.
  - Controller and processor both involved in the processing = default to controller’s lead SA.
Supervision and enforcement

SA procedures

- Cooperation
- Mutual assistance
- Joint operations
- Consistency mechanism
- Dispute resolution
- Urgency procedure

Session notes

SA procedures (Chapter VII, GDPR)
- Procedures intended to support cooperation between SAs and consistent GDPR application across member states
- Procedures heavily summarised here
- Cooperation
  - Between lead SA and other concerned SAs to reach consensus
- Mutual assistance
  - Provision of relevant information between supervisory authorities
- Joint operations
  - Joint SA investigations and enforcement measures of controllers or processors in several member states or when data subjects are in more than one member state
- Consistency mechanism
  - Specific collaborative process between SAs, Commission and European Data Protection Board for adopting certain measures and ensuring consistent GDPR application
- Dispute resolution
  - Mechanism to dispute a decision (if not jointly agreed upon by SA)
  - Issuance of binding decisions
- Urgency procedure
  - For the immediate adoption of provisional measures within a member state
Supervision and enforcement

The European Data Protection Board (EDPB)

- Composition
- Independence
- Tasks

Session notes

European Data Protection Board (EDPB) (Section 3, GDPR)
- Replaces Article 29 Working Party
- Composition
  - Representatives of every member state’s SA
    - Each of the 30 member states of the EEA will appoint representative to sit on the EDPB
    - Only representatives from the 27 EU member states may actively participate
  - Presided over by chair elected by EDPB representatives
  - Participation from European Data Protection Supervisor (EDPS) and representatives of Commission
    - EDPS limited voting rights (more on EDPS on following slide)
    - Commission no voting rights
- Independence
  - EDPB must act independently
Chat: Let’s talk about...
Is the Article 29 Working Party’s guidance still valid under the GDPR?
Session notes

The European Data Protection Supervisor (EDPS)

- The data protection regulator for EU as an entity
- **Supervision and enforcement**
  - Monitoring personal data processing of EU bodies (Commission, Council, Parliament, etc.)
  - Checking processing operations that pose high risk to data subjects (before processing)
  - Dealing with complaints
  - Making inquiries
  - Consulting
- **Consultation**
  - Advising community
  - Intervening in cases before CJEU
- **Cooperation**
  - Cooperating with supervisory authorities and supervisory data protection bodies (e.g., Europol)
- **Secretariat of the EDPB**
- Oversight of Eurodac
Supervision and enforcement
Remedies, liabilities, penalties

- Data subjects’ rights
- Liability of controllers and processors
- Administrative fines
- Administrative penalties

Module 11: Supervision and enforcement

Session notes

Remedies, liabilities, penalties (Articles 77-84)
- Data subjects’ rights
  - To lodge complaint with SA
  - To judicial remedy against a controller/processor or SA
- Liability of controllers and processors for damages caused by GDPR infringements
  - Compensation to individuals who suffer damages
- Administrative fines (see following slide)
- Additional penalties
  - Determination of penalties in addition to administrative fees made by member states
Let’s talk about...

What is the maximum amount in administrative fines that a controller or processor may receive for a GDPR infringement?

Chat: Let’s talk about...

What is the maximum amount in administrative fines that a controller or processor may receive for a GDPR infringement?
Session notes

Administrative fines

- Depending on several factors
  - Nature, gravity and duration of infringement
  - Nature, scope and purpose(s) of processing
  - Number of data subjects concerned
  - Level of damage and damage mitigation
  - Intent or negligence
  - Degree of responsibility (technical and organisational measures)
  - Previous infringements
  - Degree of cooperation with SA
  - Categories of personal data
  - Manner of notification
  - Compliance with measures ordered by SA
  - Adherence to approved codes of conduct/certification mechanisms

- Up to €20,000,000 or 4% of total turnover (whichever is higher) for infringements of principles, data subjects’ rights, international data transfers, obligations of member state law and noncompliance with SA’s order
  - Infringements tend to be more substantive

- Up to €10,000,000 or 2% of total turnover (whichever is higher) for infringements of most other obligations
  - Infringements tend to be more administrative
Session notes

Enforcement action: CNIL levies $57M fine on Google for GDPR violations (2019)

The French data protection authority, the CNIL, announced it fined Google $57 million ‘in accordance with the General Data Protection Regulation … for lack of transparency, inadequate information and lack of valid consent regarding the ads personalisation’. The CNIL said the ‘“one-stop-shop mechanism” was not applicable’, allowing it, along with other DPAs, to be a competent authority. According to the Wall Street Journal, Ireland’s Data Protection Commission said, ‘Google until now hasn’t met its criteria for having an establishment in Ireland, because its U.S. entity was responsible for processing EU users’ data, rather than its Irish unit’. The DPC will ‘become Google’s lead [DPA] in the EU for most matters’. Brave’s Johnny Ryan said the ‘CNIL’s decision is very significant because it means that Google must stop building advertising profiles about people until it has properly told them what it is doing and received their consent’.
Session notes

Former Article 29 Working Party’s ‘Guidelines on the Application and Setting of Administrative Fines’

- SAs will consider the ‘nature, gravity and duration of the infringement’
- Some cases may only trigger a reprimand
  - Where the infringement ‘does not pose a significant risk to the rights of the data subjects concerned and does not affect the essence of the obligation in question’ or if a fine would impose a ‘disproportionate burden’ on a ‘natural person’
- Factors to consider when determining the potential size of a fine:
  - Number of data subjects involved: The more people affected, the bigger the fine
  - Purpose of the processing: SAs will examine how the organisation has addressed the purpose limitation principle—purpose specification and compatible use
  - Damage suffered by data subjects: While SAs are not competent to award compensation to the data subjects themselves, they are encouraged to consider the damage suffered, or likely to be suffered, as suggested by examples of the ‘risks to rights and freedoms’ in Recital 75
  - Duration of the infringement: Fines are more likely if the violation is a result of negligent or intentional behaviour; actions taken ‘in spite of advice from the [DPO]’ may be considered ‘intentional’
Review question

NOTE: Review questions are intended to help reinforce key topics covered in the module. They are not meant to represent actual certification exam questions.

1. Who does the GDPR task with promoting, monitoring and enforcing the GDPR?

   A. Controllers
   B. Processors
   C. Supervisory authorities
   D. The European Data Protection Supervisor
2. How many active participants will the European Data Protection Board have?

A. 30
B. 27
C. 21
D. 38
Review question

3. Which mechanism facilitates the provision of relevant information between supervisory authorities?

A. Cooperation
B. Mutual assistance
C. Consistency mechanism
D. Urgency procedure
Review question

4. Which mechanism facilitates a specific collaborative process between supervisory authorities, the Commission and the European Data Protection Board for adopting certain measures and ensuring consistent GDPR application?

A. Cooperation  
B. Joint operations  
C. Consistency mechanism  
D. Dispute resolution
Questions?
Thank you!
Appendix
EUROPEAN DATA PROTECTION:
REVIEW QUESTIONS ANSWER KEY

MODULE 1
1. Which of the following data protection milestones is a treaty amongst member states of the Council of Europe?
   • Convention 108
2. Which of the following data protection milestones applies to public electronic communications services and networks?
   • ePrivacy Directive
3. The European Convention on Human Rights is a product of which institution?
   • The Council of Europe
4. Which role best describes the European Parliament?
   • Is engaged in legislative development

MODULE 2
1. What is the function of the four-step test?
   • Determine if data qualifies as personal data
2. Which criteria are used to identify personal data? Select all that apply.
   • ‘any information’
   • ‘relating to’
   • ‘an identified or identifiable’
   • ‘natural person’
3. Select the types of personal data elements that belong to special categories under the GDPR.
   • Personal data revealing political opinions
   • Personal data revealing religious or philosophical beliefs
   • Genetic data used to uniquely identify a natural person
4. True or false: Anonymising personal data is always possible.
   • False
5. True or false: Pseudonymous data is protected by the GDPR.
   • True
6. Is the collection and use of device dynamic IP addresses to allow data on a website to be transferred to the correct recipient considered personal data? Why or why not?
   • In Patrick Breyer v Bundesrepublik Deutschland, the CJEU ruled that dynamic IP addresses were capable of constituting personal data. A person could be indirectly identified if the IP addresses were combined with data help by ISPs.
MODULE 3

1. True or false: A data controller may be a natural person or a legal entity, while a data processor must be a legal entity.
   - False

2. True or false: A contract protects a processor from being held to the same legal obligations as the controller.
   - False

3. True or false: A processor may decide where and how to process personal data.
   - False

4. What actions can a controller take to manage vendor risk?
   - Choose reliable processors
   - Maintain quality control and compliance throughout the duration of the arrangements
   - Frame the relationship in a contract (or other legally binding act)

MODULE 4

1. What is data processing?
   - Any action performed upon data

2. What are the criteria used to determine the territorial scope of the GDPR? Select all that apply.
   - Processing of personal data when a controller or processor is established in the EU
   - Processing of personal data of EU subjects relating to offering goods or services or monitoring behaviour
   - Processing of personal data by a controller not established in the EU but in a place where member state law applies

3. True or false: Exclusions to the material scope of the GDPR should be interpreted broadly.
   - False

4. Which exception to the prohibition on processing special categories of data must be explicit?
   - Consent

MODULE 5

1. Which of the following data subjects’ rights provides data subjects with entitlements to certain information, obtainable from the controller upon request?
   - Right of access

2. The right of access grants data subjects access to which of the following types of information? Select all that apply.
   - The purpose of the processing
   - Retention periods
   - Recipients of the personal data
3. Which is not listed by the GDPR as a method for restricting processing of personal data?
   - Disabling the data management system

4. Under which categories may a data subject object to processing personal data? Select all that apply.
   - Direct marketing
   - Public interest or legitimate interest
   - Research or statistical purposes

5. What is profiling?
   - A form of automated decision-making

**MODULE 6**

1. True or false: A controller may charge an administrative fee to data subjects if they request that the information provision be in an oral format.
   - False

2. True or false: The transparency principle states that detail is more important than conciseness in a privacy notice.
   - False

3. What information must be provided to data subjects when the controller’s necessity is being used as the legal basis for processing?
   - Controller’s legitimate interest

4. What information must be provided to data subjects when the personal data that will be processed was collected indirectly?
   - Source of the data

5. What information must be provided to data subjects when their personal data will be shared with an outside organisation to provide them with a promised service?
   - Recipients of the data

6. What information must be provided to data subjects in all circumstances? Select all that apply.
   - Purpose of processing
   - Data subjects’ rights
   - Identity of the controller

7. True or false: Information provision is required, even if it necessitates disproportionate effort.
   - False
MODULE 7
1. Arrange the options for international data transfers in the order that they should be considered.
   - Adequacy decisions
   - Appropriate safeguards
   - Derogations
2. Which of the following options for international data transfers is a determination by the European Commission that a third country has achieved an EU-level of personal data protection?
   - Adequacy decision
3. Which of the following countries have been deemed adequate by the European Commission? Select all that apply.
   - Argentina
   - New Zealand
   - Switzerland
   - Uruguay
4. Which of the following are appropriate safeguards for international data transfers? Select all that apply.
   - Binding corporate rules
   - Standard contractual clauses
   - Approved codes of conduct or certification mechanisms
5. Which appropriate safeguards allow large multinational companies to adopt a policy suite with rules for handling personal data?
   - Binding corporate rules
6. True or false: Criteria for derogations are strict and should be interpreted narrowly.
   - True

MODULE 8
1. Which types of laws should be considered when processing employees’ personal data? Select all that apply.
   - Local employment law
   - EU data protection law
   - Member state data protection law
2. Under the GDPR, which legal basis for processing personal data would be difficult to use for processing employee data?
   - Consent
3. True or false: Some employers may be required to consult with works councils and/or trade unions to process employees’ personal data.
   - True

4. True or false: Some employers may be required to consult with works councils and/or trade unions to process employees’ personal data.
   - True

5. True or false: BYOD policies are designed to protect employees’ personal data only.
   - False

6. The ePrivacy Directive governs the processing of which types of data? Select all that apply.
   - Location data
   - Content data
   - Traffic data

7. True or false: The ePrivacy Directive governs the processing of data through both private and public carriers and communications networks.
   - False

8. True or false: Under the GDPR, individuals have the absolute right to object to any form of direct marketing at any time.
   - True

9. Which forms of marketing are subject to the ePrivacy Directive? Select all that apply.
   - Telephone marketing
   - Electronic mail marketing

10. Which of the following parties involved in online behavioural advertising may qualify as a data controller? Select all that apply.
    - An ad network
    - A website publisher
    - An advertiser

**MODULE 9**

1. CIAR stands for _____.
   - Confidentiality, integrity, availability, resilience

2. True or false: A processor is responsible for implementing appropriate technical and organisational measures to keep personal data secure.
   - True

3. A controller must notify the SA of a personal data breach if _____.
   - The breach is likely to result in a risk for the rights and freedoms of natural persons.
MODULE 10

1. True or false: Both controllers and processors have accountability obligations under the GDPR.
   - True

2. True or false: Data protection by design begins before processing and incorporates data protection considerations into the planning phase.
   - True

3. What are the main values of a data protection impact assessment (DPIA)? Select all that apply.
   - Incorporating data protection considerations into organisational planning
   - Demonstrating compliance to supervisory authorities

4. True or false: The GDPR requires controllers to always contact the SA following a DPIA and before processing personal data.
   - False

5. True or false: The GDPR requires a data protection policy to be used ‘where proportionate in relation to processing activities’.
   - True

6. Which of the following must be included in controllers’ personal data processing records but not in processors’ records?
   - Purposes of processing

7. True or false: The data protection officer must be an expert in data protection law and practices.
   - True

8. Which of the following are circumstances that require an organisation to appoint a DPO? Select all that apply.
   - The controller is a public authority.
   - The core activities of the controller or processor include regular and systematic monitoring of data subjects on a large scale.
   - The core activities of the controller or processor consist of large-scale processing of special categories of data.

MODULE 11

1. Who does the GDPR task with promoting, monitoring and enforcing the GDPR?
   - Supervisory authorities

2. How many active participants will the European Data Protection Board have?
   - 27

3. Which mechanism facilitates the provision of relevant information between supervisory authorities?
   - Mutual assistance
4. Which mechanism facilitates a specific collaborative process between supervisory authorities, the Commission and the European Data Protection Board for adopting certain measures and ensuring consistent GDPR application?

- *Consistency mechanism*
EUROPEAN DATA PROTECTION RESOURCES

PRIMARY RESOURCES

"2018 Reform of Data Protection Rules." European Commission Website.


General Data Protection Regulation (full text)
Glossary of Privacy Terms: https://iapp.org/resources/glossary/

Module 1

http://news.bbc.co.uk/hi/english/static/in_depth/europe/2001/inside_europe/eu_institutions/flow_chart.stm

European Commission GDPR guidance website:


IAPP “EU Member State GDPR Derogation Implementation Tracker”:


Module 3


Module 4


Module 5


Module 6


Module 7


Module 8


Ethic guidelines for Trustworthy AI: https://iapp.org/media/pdf/resource_center/AIEthicsGuidelinespdf.pdf

Module 9


Module 10


Module 11


I. Introduction to European Data Protection

A. Origins and Historical Context of Data Protection Law

1. Rationale for data protection
   - Module 1
2. Human rights laws
   - Module 1
3. Early laws and regulations
   - Module 1
4. The need for a harmonised European approach
   - Module 1
5. The Treaty of Lisbon
   - Module 1
6. A modernised framework
   - Module 1

B. European Union Institutions

1. Council of Europe
   - Module 1
2. European Court of Human Rights
   - Module 1
3. European Parliament
   - Module 1
4. European Commission
   - Module 1
5. European Council
   - Module 1
6. European Court of Justice of the European Union
   - Module 1

C. Legislative Framework

1. The Council of Europe Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data of 1981 (The CoE Convention)
   - Module 1
2. The EU Data Protection Directive (95/46/EC)
   - Module 1
3. The EU Directive on Privacy and Electronic Communications (2002/58/EC) - (ePrivacy Directive) - as amended
   - Module 1, Module 8
   - Module 1
5. European data retention regimes
   - Module 1
   - All modules

II. European Data Protection Law and Regulation

A. Data Protection Concepts
| 1. Personal data                      | Module 2 |
| 2. Sensitive personal data           | Module 2 |
| 3. Pseudonymous and anonymous data  | Module 2 |
| 4. Processing                        | Module 4 |
| 5. Controller                        | Module 3 |
| 6. Processor                         | Module 3 |
| 7. Data subject                      | Module 3 |

**B. Territorial and Material Scope of the General Data Protection Regulation**

| 1. Establishment in the EU           | Module 4 |
| 2. Non-establishment in the EU       | Module 4 |

**C. Data Processing Principles**

| 1. Fairness and lawfulness           | Module 4 |
| 2. Purpose limitation                | Module 4 |
| 3. Proportionality                   | Module 4 |
| 4. Accuracy                          | Module 4 |
| 5. Storage limitation (retention)    | Module 4 |
| 6. Integrity and confidentiality     | Module 4 |

**D. Lawful Processing Criteria**

| 1. Consent                           | Module 4 |
| 2. Contractual necessity             | Module 4 |
| 3. Legal obligation, vital interests and public interest | Module 4 |
| 4. Legitimate interests               | Module 4 |
| 5. Special categories of processing  | Module 4 |

**E. Information Provision Obligations**

<p>| 1. Transparency principle            | Module 6 |
| 2. Privacy notices                   | Module 6 |
| 3. Layered notices                   | Module 6 |</p>
<table>
<thead>
<tr>
<th>F. Data Subjects’ Rights</th>
<th>Module 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Access</td>
<td></td>
</tr>
<tr>
<td>2. Rectification</td>
<td></td>
</tr>
<tr>
<td>3. Erasure and the right to be forgotten (RTBF)</td>
<td></td>
</tr>
<tr>
<td>4. Restriction and objection</td>
<td></td>
</tr>
<tr>
<td>5. Consent, including right of withdrawal</td>
<td></td>
</tr>
<tr>
<td>6. Automated decision making, including profiling</td>
<td></td>
</tr>
<tr>
<td>7. Data portability</td>
<td></td>
</tr>
<tr>
<td>8. Restrictions</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>G. Security of Personal Data</th>
<th>Module 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Appropriate technical and organisational measures</td>
<td></td>
</tr>
<tr>
<td>2. Breach notification</td>
<td></td>
</tr>
<tr>
<td>3. Vendor management</td>
<td>Module 3</td>
</tr>
<tr>
<td>4. Data sharing</td>
<td>Module 3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>H. Accountability Requirements</th>
<th>Module 3, Module 10</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Responsibility of the controllers and processors</td>
<td>Module 10</td>
</tr>
<tr>
<td>2. Data protection by design and by default</td>
<td>Module 10</td>
</tr>
<tr>
<td>3. Documentation and cooperation with regulators</td>
<td>Module 10</td>
</tr>
<tr>
<td>4. Data protection impact assessment</td>
<td>Module 10</td>
</tr>
<tr>
<td>5. Mandatory data protection officers</td>
<td>Module 10</td>
</tr>
<tr>
<td>6. Auditing of privacy programs</td>
<td>Module 10</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>I. International Data Transfers</th>
<th>Module 7</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Rationale for prohibition</td>
<td></td>
</tr>
<tr>
<td>2. Safe jurisdictions</td>
<td></td>
</tr>
<tr>
<td>3. Safe Harbor and Privacy Shield</td>
<td></td>
</tr>
<tr>
<td>4. Model contracts</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>5. Binding Corporate Rules (BCRs)</td>
<td>Module 7</td>
</tr>
<tr>
<td>6. Codes of Conduct and Certifications</td>
<td>Module 7</td>
</tr>
<tr>
<td>7. Derogations</td>
<td>Module 7</td>
</tr>
<tr>
<td>8. Transfer impact assessments (TIAs)</td>
<td>Module 7</td>
</tr>
<tr>
<td><strong>J. Supervision and enforcement</strong></td>
<td></td>
</tr>
<tr>
<td>1. Supervisory authorities and their powers</td>
<td>Module 11</td>
</tr>
<tr>
<td>2. The European Data Protection Board</td>
<td>Module 11</td>
</tr>
<tr>
<td>3. Role of the European Data Protection Supervisor (EDPS)</td>
<td>Module 11</td>
</tr>
<tr>
<td><strong>K. Consequences for GDPR violations</strong></td>
<td></td>
</tr>
<tr>
<td>1. Process and procedures</td>
<td>Module 11</td>
</tr>
<tr>
<td>2. Infringements and fines</td>
<td>Module 11</td>
</tr>
<tr>
<td>3. Role of the European Data Protection Supervisor (EDPS)</td>
<td>Module 11</td>
</tr>
<tr>
<td><strong>III. Compliance with European Data Protection Law and Regulation</strong></td>
<td></td>
</tr>
<tr>
<td><strong>A. Employment Relationship</strong></td>
<td></td>
</tr>
<tr>
<td>1. Legal basis for processing of employee data</td>
<td>Module 8</td>
</tr>
<tr>
<td>2. Storage of personnel records</td>
<td>Module 8</td>
</tr>
<tr>
<td>3. Workplace monitoring and data loss prevention</td>
<td>Module 8</td>
</tr>
<tr>
<td>4. EU Works councils</td>
<td>Module 8</td>
</tr>
<tr>
<td>5. Whistleblowing systems</td>
<td>Module 8</td>
</tr>
<tr>
<td>6. ‘Bring your own device’ (BYOD) programs</td>
<td>Module 8</td>
</tr>
<tr>
<td><strong>B. Surveillance Activities</strong></td>
<td></td>
</tr>
<tr>
<td>1. Surveillance by public authorities</td>
<td>Module 8</td>
</tr>
<tr>
<td>2. Interception of communications</td>
<td>Module 8</td>
</tr>
<tr>
<td>3. Closed-circuit television (CCTV)</td>
<td>Module 8</td>
</tr>
<tr>
<td>4. Geolocation</td>
<td>Module 8</td>
</tr>
<tr>
<td>5. Biometrics/facial recognition</td>
<td>Module 8</td>
</tr>
<tr>
<td><strong>C. Direct Marketing</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>1.</td>
<td>Telemarketing</td>
</tr>
<tr>
<td>2.</td>
<td>Direct marketing</td>
</tr>
<tr>
<td>3.</td>
<td>Online behavioural targeting</td>
</tr>
</tbody>
</table>

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>D.</td>
<td>Internet Technology and Communications</td>
<td></td>
</tr>
<tr>
<td>1.</td>
<td>Cloud computing</td>
<td>Module 8</td>
</tr>
<tr>
<td>2.</td>
<td>Web cookies</td>
<td>Module 8</td>
</tr>
<tr>
<td>3.</td>
<td>Search engine marketing (SEM)</td>
<td>Module 8</td>
</tr>
<tr>
<td>4.</td>
<td>Social networking services</td>
<td>Module 8</td>
</tr>
<tr>
<td>5.</td>
<td>Artificial Intelligence (AI)</td>
<td>Module 8</td>
</tr>
<tr>
<td>a.</td>
<td>machine learning</td>
<td>Module 8</td>
</tr>
<tr>
<td>b.</td>
<td>ethical issues</td>
<td>Module 8</td>
</tr>
</tbody>
</table>
Ready to get certified?
Leave the stress and pass the test

Providing you with respected credentials requires a rigorous certification process that includes demanding exams. IAPP exams have a reputation for being difficult to pass on the first try. We strongly recommend careful preparation, even for degreed professionals who have passed other certification tests.

Preparation makes all the difference. In general, we recommend that you train and study for a minimum of 30 hours.

We want you to succeed. Please take advantage of this advice and IAPP resources to get through exams with as little anxiety as possible.

Tips for effective studying
Completing a training course does not guarantee passing an exam. Additional preparation is essential, so:

• **Self-assess**—The IAPP offers two resources for determining how ready you are for the exam:
  1. The **body of knowledge** is an outline of the information covered in the exam. Use it to identify topics you are and are not familiar with.
  2. The **exam blueprint** tells you how many questions to expect on each topic. Use it to map out a study strategy—allowing more time for topics with many questions, for example.

You can find links to the exam blueprints and bodies of knowledge at [iapp.org/certify/get-certified/](http://iapp.org/certify/get-certified/).

• **Use your textbook properly**—Textbooks are included with purchase of in-person and online training, and are also sold separately through the IAPP store at [iapp.org/store/books/](http://iapp.org/store/books/).
Certified Information Privacy Professional - Europe (CIPP/E) Certification Exam Details

This information sheet is for anyone interested in participating in CIPP/E certification.

Registration
Examinations are offered year-round.

- To purchase an exam, visit the IAPP store: iapp.org/store/certifications
- Exams must be scheduled AND completed within one year of purchase
- For more information, please visit Pearson Vue’s website: pearsonvue.com/iapp

Cost
- First-time test taker: $550
- Retake exams: $375

Preparation The IAPP offers many additional tools to help you prepare for certification at iapp.org/certify/get-certified/cippe.

- List of Authoritative Resources
- Body of Knowledge - Lists possible exam topics
- Exam Blueprint - Shows relative weight of topics on the exam
- Glossary of Privacy Terms

Get your free IAPP Study Guide at iapp.org/certify/free-study-guides and we encourage potential test takers to read our Certification Candidate Handbook here: iapp.org/certify/get-certified/.

Structure
All examinations consist of multiple choice questions. Some items require reading a short scenario, then answering questions relating to that scenario.

- 90 questions
- Two hours 30 minutes allotted time

Scoring
All IAPP Certification Exams are pass-fail. If you do not pass, you will receive a scoring breakdown by topic to help identify areas requiring increased study should you choose to retake the exam. A 30-day wait is required from the date of your previous exam before testing again.

If you have additional questions or concerns, please contact certification@iapp.org.
IAPP Member Benefits  At-a-Glance

- Daily and weekly e-publications summarizing top privacy news
- Discounted rates on education products and programs, including study materials for our globally recognized certification programs, and annual conferences and events
- *The Privacy Advisor*, the IAPP’s monthly members-only newsletter
- Professional networking opportunities, including free KnowledgeNet chapter meetings to keep you connected in your local community
- Privacy salary surveys that benchmark compensation trends, roles and functions among privacy departments
- Privacy job postings
- Access to members-only tools, research, articles and more in the IAPP’s online Resource Center
- The IAPP Membership Directory, an online tool that allows you to search for and network with other IAPP members
- Free web conferences
- Access to the *Privacy Tracker* blog
- Cooperative programs with other national and international organizations
- Advocacy for the privacy profession

**News**
You are busy. We make it easy to stay on top of the headlines.

**Certify**
IAPP certification is what employers want. We can help you advance your career and increase your earning potential.

**Learn**
10+ free web conferences give you instant access to the latest and greatest in privacy.

**Connect**
It is all about who you know. Targeted online and face-to-face networking opportunities give you access to the people you want to meet.

**Resources**
The newly revamped Resource Center is a one-stop-shop for practical tools and research to help you tackle your biggest challenges.
Start by reading the table of contents. Note which topics are new to you. That will give you a feel for how much study and review time you need. When you start reading:

1. Highlight important points in each chapter.
2. Copy out key passages; it will help you remember them.
3. Review each chapter to make sure you have captured the key points before moving on.

- **Create flashcards**—As you read your textbook, articles, web pages, etc., copy new terms onto notecards. Write their definitions on the other side. Quiz yourself. Use the IAPP’s glossary of privacy terms to look up unfamiliar terms and make flash cards of them as well.
- **Form a study group**—Discussing the material with your coworkers and colleagues is a great way to remember material and understand it more deeply.
- **Learn in context**—It is easier and more interesting to learn a subject you are going to use in real life. IAPP publications and resources show how privacy affects our lives and businesses. Get familiar with privacy news and issues by signing up for the IAPP’s Daily Dashboard, Privacy Advisor, and Europe Data Protection Digest.
- **Use questions to find answers**—Every training course comes with sample questions to help you review what you have studied and identify weak areas. Re-read notes and chapters on those subjects. Ask your study partners questions. Search for articles that approach the subject from different directions.

Find this information, with hyperlinks to the relevant resources mentioned above, on the IAPP website at [iapp.org/certify/prepare](http://iapp.org/certify/prepare). Good luck!
Certificate of Attendance

This certificate is presented to:

_________________________________________________
Participant’s Name

for successfully completing the:
European Data Protection Training

________________________________
City/State

________________________________
Date

Type of Event: Training-Live Format
Total Hours of Education: 13

J. Trevor Hughes, CIPP
President & CEO, IAPP