Training Fiche ESSEI

|  |  |
| --- | --- |
| Title | What is GDPR? |
| Training Area | *Please select one or more of the following:*   |  |  | | --- | --- | | Online Security | *X* | | Cultural and Media Literacy |  | | Economic Transactions |  | | Personal Data Protection |  | | Digital Identity and online reputation |  | |
| Keywords (meta tag) | GDPR, privacy, data protection |
| Provided by | ESSEI asbl |
| Language | ENG |
| Objectives / goals / learning outcomes | |
| At the end of this module you will be able to:   * Familiarise with the GDPR   *Background, scale and scope…*   * Gain awareness on your (digital) rights   *The right to be forgotten*   * Comprehend what cookies are what is their scope   *When they are harmful and when they are not…* | |
| Description | |
| Have you ever noticed that whenever you try to access a website, a big disclaimer pops up requesting you to read carefully (and accept eventually) their cookie policy?  What is a cookie and what is this disclaimer about? Why is the WWW so concerned about terms and conditions of your privacy and (digital) identity?  While surfing on the Internet, you might have come across – or read about – something known as GDPR…but in practice, what is GDPR? | |
| Contents arranged in 3 levels | |
| **Module 1: What is GDPR?**  Have you ever noticed that whenever you try to access a website, a big disclaimer pops up requesting you to read carefully (and accept eventually) their cookie policy?  What is a cookie and what is this disclaimer about? Why is the www so concerned about terms and conditions of your privacy and (digital) identity?  While surfing on the Internet, you might have come across – or read about – something known as GDPR…  **Unit 1.: General Overview**  **Section 1.1 For beginners**  The GDPR (General Data Protection Regulation) is an EU Parliament and EU Council regulation of April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.  **Section 1.2 Brief disclaimer – what is a Regulation in EU law?**  Together with Directives, Decisions, Recommendations and Opinions, Regulations represent of the types of EU legislation – legal acts of different binding degrees to which all (or some) Member States should comply with.  Regulations are the ones with at higher binding degree and they must be applied in their entirety across EU.  **Section 1.3 About general scale and scope of GDPR**  In the formal policy document, it is stated that:   1. [GDPR] lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data. 2. [GDPR] protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.   **Section 1.4 Who must comply with GDPR?**  The whole point of this regulation is to protect EU’s citizens personal data. As such, any organisation operating in EU territories must comply with GDPR.  The regulation applies to ALL organisation, regardless of their juridical status (public institutions, private sectors’ representatives and third sector) and their country of origin, as long as they operate in EU territories (this is the case of tech giants from US such as Facebook, Google, Amazon, etc.).  **Unit 2: Key highlights**  In order to have a comprehensive understanding of GDPR, it is important to pinpoint a couple of terms around which the regulation revolves. These includes:   * Seven principles of data protection * Eight privacy rights that must be protected (and supported) * Glossary of specific references used by the Regulation   **Section 2.1 Glossary and reference terms – Article 4, Definitions (1)**  Personal data → Any information relating to an identified or identifiable natural person (“data subject”); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.  **Section 2.2 Glossary and reference terms – Article 4, Definitions (2)**  Processing → Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as: collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.  **Section 2.3 Glossary and reference terms – Article 4, Definitions (3, 4)**  Restriction of Processing → The marking of stored personal data with the aim of limiting their processing in the future.  Profiling → Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.  **Section 2.4 Glossary and reference terms – Article 4, Definitions (7, 8)**  Controller → The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.  Processor → A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.  **Section 2.5 Glossary and reference terms – Article 4, Definitions (11, 12)**  Consent → Any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.  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.  **Section 2.6 Seven principles of data protection – Chapter 2, Article 5**   1. Lawfulness, fairness and transparency of data processing 2. Purpose limitation – data should be *collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes* 3. Data minimisation – data should be *adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed* 4. Accuracy – data should be *accurate and, where necessary, kept up to date* 5. Storage limitation – data should be *kept in a form which permits identification of data subjects for no longer than is necessary* 6. Integrity and confidentiality – data should be *processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing* 7. Accountability – The controller shall be responsible for, and be able to demonstrate compliance with 1 to 6   **Section 2.7 Eight privacy rights that must be protected – Chapter 3, Article 12 – 23**   1. Citizens have the right to be informed about the processing of their data form third parties. The controller shall take appropriate measures to provide any information […] relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form […]. 2. Citizens have the right to access their data. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, access to the personal data and the following information 3. Citizens have the right to rectification of their data. The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. 4. Citizens have the right to be forgotten. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her 5. Citizens have the right to restrict processing of their data. 6. Citizens have the right to the portability of their data. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided 7. Citizens have the right to object their data. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing 8. Citizens have rights in relation to automated decision making and 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   **Unit 3: Implications for citizens**  **Section 3.1 When organisations are allowed to process your data**  There are some specific scenarios in which organisations – upon full compliance with GDPR – are allowed to process your data (processing in the sense of Art. 4).  Article no. 6 of the Regulations lists all instances in which organisations can in fact “look into” your personal data.  These conditions fall under six domains…   1. There is specific consent (unambiguous) by the subject this data belongs to 2. The subject is entering into a contract – and the organisation is entitled to a background check of personal information 3. The organisation process data to comply with further legal obligations 4. In the case data processing is instrumental *to protect the vital interests of the data subject or of another natural person* 5. In the case data processing is instrumental *for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller* 6. Any other case in which there is legitimate interest by the organisation   **Section 3.2: Legitimate interest**  Scenario no. 6 is more susceptible to free interpretation than all the others. If the given interest is legitimate or not, depends on its explicit conflict (or not) with fundamental rights and freedoms of data subjects.  The label of legitimate interest can gain also other shapes and forms in “sensitive” cases: people with criminal records, children and other vulnerable categories…  **Section 3.3: Website cookies**  The most typical example in which you agree on to the processing of your (digital) data is when you accept cookies before browsing any website you want access to.  Cookies are designed to improve your browsing experience and allow website’s owner(s) to keep you signed in, store your preferences, and provide you with locally relevant content that is thematic to your interests.  Due to the clear conflict of interest, after GDPR website’s owners become increasingly concerned about your awareness on this tool.  **Section 3.4: How many cookies are out there?**  This depends on:   * DURATION * PROVENANCE * PURPOSE   **DURATION**   * Sessions cookies – they expire as soon as you end your session * Persistent cookies – they remain on your hard drive as long as you don’t delete them “manually”. Persistent cookies have the expiration date embedded into their programming code. Technically they should not last more than 12 months, but in practice they might live much longer   **PROVENANCE**   * First-party cookies – they are put on your IT device (laptop, phone, etc.) by the very same website your accessing into * Third-party cookies – they are put on your IT device by – typically – an advertiser that has a formal agreement with the website’s owner(s)   **PURPOSE**   * Strictly necessary – cookies that are functional (essential) for your browsing experience (save the item that you want to by into the shopping list) * Preferences – cookies that allow website’s owners to retain information that will improve and facilitate your next visit of the website (save log-in credentials) * Statistics – relatively harmless, these cookies help website’s owners in better understating what users like and look into * Marketing – typically of third-party provenance, these cookies help advertisers in collecting information about, for instance, purchase behaviour of customers   **Section 3.5: Should you accept cookies?**  Technically speaking, you’re not forced to accept cookies. The GDPR is designed to make you aware of their existence and usage by website’s owner(s) and third parties.  This helps you to make better informed decisions on who you’re giving your data and what for…  …however, if that is the case, website’s owner(s) might retain the right to block you from accessing their website or to limit its functionalities and your overall browsing’s experience.  **Section 3.6: Cookies are not a threat when…**   * The website you’re visiting is highly reliable (i.e., your Facebook account) * They help you improving your user’s experience (i.e., online shopping, online banking, etc.) * They save you time and resources – specifically when repeatedly logging in to your go-to websites (i.e., email account)   **“Red flags”**   * The website you’re visiting is NOT encrypted – the lock icon beside the URL is not locked Per se, these websites are not dangerous but they might not be prepared to data breaches neither…keep an eye open. * Third-parties’ cookies. Again, these cookies are not dangerous, but if you’re particularly concerned about your (digital) privacy, you might not like the idea of someone looking into your data. * Whenever your antivirus spots suspicious activities. * In any case you need to provide the website with highly-sensitive information (bank account, scan and copy of ID, etc.).   ***FOR INSTANCE: Website cookies, EU Commission’s website:***  …the EU Commission website relies for the most on first-parties cookies of three main kinds:   1. **Store Visitors Preferences**   **Accessible by IT team, they keep track of:**   * Various user-website interfaces (*how helpful the site content was*) * Previous acceptance (or not) of website cookies  1. **Operational cookies**   **Functional for the operability of certain webpages**  ***Authentication & Technical cookies***  These are stored when you log in to a Commission site, using our authentication service (EU Login). When you do this, you accept the associated privacy policy.   1. **Analytics cookies**   **Purely for internal research and for the assessment of performance parameters**   * How users interact with the website (as anonymous users) * Not shared with third parties * People is free to refuse them   ***FOR INSTANCE: How can you manage cookies?***  Remove cookies from your device → by cleaning the history of your browser  Manage site-specific cookies → by proactively filtering the cookies that you allow and don’t  Blocking cookies → by setting-up you browser to the most “advanced” standards  **Section 3.7: *What if you wish to take action to protect your personal data?***   1. Submit a complain to your national Data Protection Authority (DPA) 2. Take legal action against the “offender” 3. Take legal action against the DPA   Source: [What should I do if I think that my personal data protection rights haven’t been respected?, EU Commission](https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/redress/what-should-i-do-if-i-think-my-personal-data-protection-rights-havent-been-respected_en)  ***1. Submit a complain to your national*** [***Data Protection Authority (DPA)***](https://edpb.europa.eu/about-edpb/about-edpb/members_en)    ***2.Take legal action against the “offender”***  Definitely a more direct approach than the previous one…  You can be assisted by a professional (i.e., lawyer) if your think that a company or an organisation “mistreated” your personal data = non-compliance with any of the seven principles of data protection.  ***3. Take legal action against the DPA***  If you have a genuine belief that the DPA failed to represent your interests, you have the right to settle the case before a court. This is the case when:   1. You are not satisfied with the answer / reply / feedback you have been given 2. You don’t receive updates / news on your case from the DPA within 3 months starting counting from the first day you submitted your complain to their office | |
| Contents in bullet points | |
| Module name: What is GDPR?  Unit name: General Overview  For beginners  Brief disclaimer – what is a Regulation in EU law?  About general scale and scope of GDPR  Who must comply with GDPR?  Unit name: Key highlights  Glossary and reference terms – Article 4, Definitions (1)  Glossary and reference terms – Article 4, Definitions (2)  Glossary and reference terms – Article 4, Definitions (3, 4)  Glossary and reference terms – Article 4, Definitions (7, 8)  Glossary and reference terms – Article 4, Definitions (11, 12)  Seven principles of data protection – Chapter 2, Article 5  Eight privacy rights that must be protected – Chapter 3, Article 12 – 23  Unit name: Implications for citizens  When organisations are allowed to process your data  Legitimate interest  Website cookies  How many cookies are out there?  DURATION  PROVENANCE  PURPOSE  Should you accept cookies?  Cookies are not a threat when…  “Red flags” | |
| 5 glossary entries | |
| Please refer to Unit “Key highlights” for a comprehensive and detailed overview on glossary entries relating to GDPR | |
| Bibliography and Further References | |
| n/a | |
| Five multiple-choice self-assessment questions | 1) GDPR stand for:   1. General Data Protection Regulation 2. General Data Privacy 3. General Document on People’s Rights   **Correct: A**  2) The scale and scope pf GDPR is:   1. the protection of children’s online identity 2. the protection of natural persons with regard to the processing of personal data and on the free movement of such data 3. the surveillance of cybercriminal activities   **Correct: B**  3) By “processing of data” we refer to:   * Collection, recording, organisation * Structuring, storage, adaptation * All of the above and ever more…   **Correct: C**  4) We refer to Personal Data in connection to:   * Any information relating to an identified or identifiable natural person * Physical, physiological, genetic, mental, economic, cultural or social identity of that natural person * An identifier such as a name, an identification number, location data   **Correct: A**  5) In relation to website cookies, which one of the following information is NOT true:   1. You have the right to refuse cookies 2. Cookies might improve your browsing experience 3. Third parties cookies are the least concerning cookies   **Correct: C** |
| Related Material | n/a |
| Related PPT | SOS Creativity\_ IO3 ESSEI |
| Reference Link | GDPR: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504> |
| Video in YouTube format (if any) | n/a |