****  
**STAR**  
**S**upport **T**raining **A**ctivities on the data protection **R**eform  
project-star.eu

**Draft Training materials for use by DPA**

Deliverable **D3.1**version 1.0



**István Böröcz**

**Paul De Hert**

**David Barnard-Wills**

**Filippo Marchetti**

**Gábor Kulitsán**

**Renáta Nagy**

**Júlia Sziklay**

Brussels – London – Budapest  
**28 February 2019**

distribution level: **public**



|  |  |
| --- | --- |
| trilateral-research-tri-blue-logo Macintosh HD:Users:darek:Downloads:naih-logo.png |  |

**A report prepared for the European Commission’s Directorate-General for Justice and Consumers (DG JUST).**

The STAR project (*Support Training Activities on the data protection Reform*; 2017-2019) is co-funded by the European Union under the Rights, Equality and Citizenship Programme 2014-2020 (REC-RDAT-TRAI-AG-2016) under Grant Agreement No. 769138.

The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Source of the picture on the cover page: <https://www.pexels.com/photo/person-touching-macbook-pro-1011329/>

Permanent link: <http://www.project-star.eu/training-materials>

|  |  |
| --- | --- |
| **Authors** | |
| **Name** | **Partner** |
| István Böröcz | VUB-LSTS |
| Paul De Hert | VUB-LSTS |
| Filippo Marchetti | TRI |
| David Barnard-Wills | TRI |
| Gábor Kulitsán | NAIH |
| Renáta Nagy | NAIH |
| Júlia Sziklay | NAIH |

|  |  |
| --- | --- |
| **Contributors** | |
| **Name** | **Partner** |
| Vagelis Papakonstantinou | VUB-LSTS |
| Dariusz Kloza | VUB-LSTS |
| David Wright | TRI |

|  |  |  |
| --- | --- | --- |
| **Institutional Members of the STAR Consortium** | | |
| **Member** | **Role** | **Website** |
| Vrije Universiteit Brussel (VUB) Research Group on Law, Science, Technology and Society (LSTS) | Project Coordinator | vub.ac.be/LSTS |
| Trilateral Research Ltd. (TRI) | Partner | trilateralresearch.com |
| Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) | Partner | naih.hu |

**version 1.0  
28 February 2019**

Table of Contents

[1 Introduction 8](#_Toc2270433)

[2 Training scenarios 8](#_Toc2270434)

[Scenario #1 – New staff training at a data protection authority 8](#_Toc2270435)

[Scenario #2 – Specialist training for data protection authority staff 9](#_Toc2270436)

[Scenario #3 – DPAs training for Civil servants and public sector employees 11](#_Toc2270437)

[Scenario #4 – DPAs training judges 12](#_Toc2270438)

[Scenario #5 – DPA training (new) DPOs 14](#_Toc2270439)

[Scenario #6 – DPA training (experienced or established) DPOs 15](#_Toc2270440)

[Scenario #7 - DPA training for private sector (different sectors e.g. healthcare, education) 16](#_Toc2270441)

[Scenario #8 – Training to be published by a DPA for data controllers and processors 17](#_Toc2270442)

[3 Training materials 19](#_Toc2270443)

[3.1 Presentations 19](#_Toc2270444)

[3.2 Reading materials 19](#_Toc2270445)

[3.2.1 Topic 1 – Introduction to the European Union Data Protection Regime 20](#_Toc2270446)

[3.2.2 Topic 2 - Purposes and legal grounds for processing personal data 20](#_Toc2270447)

[3.2.3 Topic 3 - The rights of the data subject and their exercise 21](#_Toc2270448)

[3.2.4 Topic 4 - Responsibilities of data controllers and processors 21](#_Toc2270449)

[3.2.5 Topic 5 – role of the DPO 21](#_Toc2270450)

[3.2.6 Topic 6 - Role of the DPA 22](#_Toc2270451)

[3.2.7 Topic 7 – technical and organizational measures 22](#_Toc2270452)

[3.2.8 Topic 8: Risk-based approach to data protection 22](#_Toc2270453)

[3.2.9 Topic 9 - Data Protection Impact Assessments 23](#_Toc2270454)

[3.2.10 Topic 10 - Data Protection Communication 23](#_Toc2270455)

[3.2.11 Topic 11 – It’s not just the GDPR - GDPR related laws and special provisions 23](#_Toc2270456)

[3.3 Operational forms 24](#_Toc2270457)

[3.3.1 Attendance sheet 24](#_Toc2270458)

[3.3.2 Evaluation questionnaire 26](#_Toc2270468)

[3.4 Compliance checklist 28](#_Toc2270469)

[3.5 Introductory guide to the GDPR 31](#_Toc2270476)

# Background to the STAR project

The STAR project (*Support Training Activities on the data protection Reform*) will provide support to the training activities of European Union (EU) Data Protection Authorities (DPAs) and data protection officers (DPOs) on the EU data protection reform, especially the General Data Protection Regulation (GDPR). The GDPR requires these two categories of data protection actors to undertake training activities (Arts 57(1) and 39(1)(b)). Each DPA developing such materials in isolation increases the overall cost, risks undermining the harmonising effect of the GDPR and puts greater pressure on its consistency mechanisms. STAR will thus provide them with necessary and efficient training materials and resources. In particular, STAR will:

1. formulate the training topics in close cooperation with stakeholders,
2. author the actual training materials,
3. validate and test them in pilot trainings.

This output will be freely and publicly available in a digital form. STAR is directly addressed to EU DPAs and DPOs; it also offers a benefit to other privacy professionals in the EU and beyond.

STAR supports the legal obligations of DPAs and DPOs to undertake training activities and, in order to facilitate their work, will provide them with ready-made, easy-to-customise and easy-to-run training materials, easily adaptable to specific training situations. STAR will also provide to the European Data Protection Board (EDPB) the common training programmes (Art 70 GDPR). The main outputs are thus the training materials and resources themselves. While their exact format and nature will be refined in cooperation with stakeholders, the following will at least be included:

1. Training scenarios for each training category,
2. A Seminars’ Topics List, based on the training scenarios,
3. Seminar Material for each one of the seminars,
4. Webinars (selected from the Seminars’ Topics List),
5. A training Handbook,
6. A takeaway reference GDPR checklist,
7. A ten-point GDPR introductory list.

# Executive summary

This deliverable contains the first iteration of the STAR training materials and supporting documents to be used by Data Protection Authorities. In particular, the deliverable contains a set of training scenarios, the training materials for DPAs to use to train DPA personnel, DPO, judges and lawyers, civil servants and public sector employees and private sector (i.e. 11 presentations in .pptx format which also contain the trainer’s guidance in the notes of each slide), reading materials for each topic, operational forms (attendance sheet and evaluation questionnaire), a compliance checklist and an introductory guide to the GDPR.

As the materials presented in this deliverable are expected to be tested and validated in real environment by DPAs, the fundamental aim of this deliverable is to provide the status of the materials on the day of submission (i.e. 28 February 2019). These materials are uploaded and are freely available on the website of the project (<http://project-star.eu/>) and will be continuously updated and refined.

# List of Abbreviations

|  |  |
| --- | --- |
| STAR | Support Training Activities on the data protection Reform |
| DPA | Data Protection Authority |
| DPO | Data Protection Officer |
| GDPR | General Data Protection Regulation |

# Introduction

This deliverable contains the first iteration of the STAR training materials and supporting documents to be used by Data Protection Authorities. In particular, the deliverable contains a set of training scenarios, the training materials for DPAs to use to train DPA personnel, DPO, judges and lawyers, civil servants and public sector employees and private sector (i.e. 11 presentations in .pptx format which also contain the trainer’s guidance in the notes of each slide), reading materials for each topic, operational forms (attendance sheet and evaluation questionnaire), a compliance checklist and an introductory guide to the GDPR.

As the materials presented in this deliverable are expected to be tested and validated in real environment by DPAs, the fundamental aim of this deliverable is to provide the status of the materials on the day of submission (i.e. 28 February 2019). These materials are uploaded and are freely available on the website of the project (<http://project-star.eu/>) and will be continuously updated and refined.

Since the materials presented in this deliverable will change continuously until the conclusion of the project, this report should not be used directly for organizing and conducting trainings.

# Training scenarios

STAR is developing GDPR training material that is intended to be useable across a range of different training scenarios. A scenario is a set of descriptive criteria that describe how the training will be delivered and set out how the training material is to be used in practice. These scenarios are not binding, but make clear our assumptions about likely ways in which the training materials developed by STAR will be used (e.g. a particular DPA may give introductory staff two days training rather than a week). These assumptions derive from the research conducted by STAR contained in Deliverables D2.2 and D2.4. A user of the STAR training material can find the scenario that most closely matches their use for the training material, and then identify any particular pedagogic approaches, practical considerations and the best ways to use the materials provided by STAR.

|  |  |
| --- | --- |
| Scenario #1 – New staff training at a data protection authority | |
| Capsule description | In this scenario, the STAR training materials are used internally within a data protection authority to introduce newly hired or recruited staff to the GDPR. |
| Trainer | Data protection authority, Staff |
| Expected knowledge of Trainer | Expected to be very high - data protection professional, with some years of experience. |
| Trainee | New staff |
| Expected knowledge of Trainee | Potentially low, including no previous data protection training. May have professional experience in other areas, but may also be a new recruit coming from education. May also include apprentices or interns. |
| Why use STAR? | To reduce the time and effort required for the trainer, and allow them to focus upon their organisational priorities.  To improve harmonisation with training delivered at other DPAs |
| Timing | One week |
| Delivery format | Classroom |
| Self-directed or trained? | Trained |
| budgeting or other constraints | Staff-time cost, premises |
| Special considerations  (including pedagogic issues) | Will probably require high tailoring to national practices to ensure that the trainee is not given generic training |
| STAR Modules to use  (include key topics, and additional topics). | * Topic 1 - Introduction to the European Union Data Protection Regime * Topic 3 - The rights of the data subject and their exercise * Topic 4 - Responsibilities of data controllers and processors * Topic 6 - The role of the Data Protection Authority |
| slides to use or remove | Need to spend some time adapting the national slides to the relevant national context |
| Supporting material to use | Decisions and procedures of the relevant DPA |
| how to specify for sector or national differences. | Add national materials in the relevant, customisable slides |
| Further adaption needed from trainer / host | Insertion of organisational branding  Insertion of any organisational best practices  Linking to any other organisational training practices  (this will likely be done once, then that adapted material re-used for several training sessions) |
| Additional reading | Please see individual slide topics |
| Other comments |  |

|  |  |
| --- | --- |
| Scenario #2 – Specialist training for data protection authority staff | |
| Capsule description | In this scenario, the STAR training materials are used internally within a data protection authority to introduce generalist staff to a specialist issue with the GDPR and take a deeper dive into a particular area. |
| Trainer | Data protection authority, Staff |
| Expected knowledge of Trainer | Expected to be very high - data protection professional, with some years of experience, and specialism in a particular domain of data protection |
| Trainee | Data protection authority, Staff |
| Expected knowledge of Trainee | Moderate to high, applied data protection experience.  The trainee has likely already completed the training in scenario #2 or equivalent. |
| Why use STAR? | To reduce the time and effort required for the trainer, and allow them to focus upon their organisational priorities.  To improve harmonisation with training delivered at other DPAs  To benefit from the specialised focus of some of the later STAR materials. |
| Timing | One to two hours. |
| Delivery format | Classroom |
| Self-directed or trained? | Trained |
| budgeting or other constraints | Staff-time cost, premises |
| Special considerations  (including pedagogic issues) | Assumes that the trainer understands why this area requires some specific focus |
| STAR Modules to use  (include key topics, and additional topics). | Uses a single module, as appropriate, from:   * Topic 5 - The role of the Data Protection Officer * Topic 7 - Data protection in practice: Technical and organisational measures * Topic 8 - Risk-based approach in the GDPR * Topic 9 - Data protection impact assessments * Topic 10 - Data protection communication * Topic 11 - It’s not just the GDPR - GDPR related laws and special provisions |
| slides to use or remove | Need to spend some time adapting the national slides to the relevant national context |
| Supporting material to use | Decisions and procedures of the relevant DPA |
| how to specify for sector or national differences. | Add national materials in the relevant, customisable slides |
| Further adaption needed from trainer / host | Trainer's experience will add to the value of the slides. |
| Additional reading | * Opinion 4/2007 of the Article 29 Data Protection Working Party of the European Commission on the concept of personal data (WP136) 20 June 2007 * Opinion 1/2010 of the Article 29 Data Protection Working Party on the concepts of controller and processor (WP169) 16 February 2010 * Handbook on European data protection law - 2018 edition <http://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law> |
| Other comments |  |

|  |  |
| --- | --- |
| Scenario #3 – DPAs training for Civil servants and public sector employees | |
| Capsule description | A formal classroom scenario where a national data protection supervisory authority provides training to civil servants and public sector employees in that country. |
| Trainer | Data protection authority |
| Expected knowledge of Trainer | High |
| Trainee | Civil servants and public sector employees |
| Expected knowledge of Trainee | Moderate to high data protection knowledge. |
| Why use STAR? | To allow quick responses to requests for training from civil servants and public sector organisations (these training sessions can be ad-hoc and responsive for many DPAs).  To reduce the time and effort required for the trainer, and allow them to focus upon their organisational priorities.  To improve harmonisation with training delivered at other DPAs  As a basis for addressing more specific questions arising from the trainee's own experiences. |
| Timing | 2 Days |
| Delivery format | Classroom |
| Self-directed or trained? | Trained |
| budgeting or other constraints | It is unlikely given the resources involved, that the DPA would be responsible for all data protection training within a national civil service. It is more likely that this is delivered to data protection specialists, who can then further disseminate this knowledge through their departments. |
| Special considerations  (including pedagogic issues) | This training may be a statutory responsibility for national DPAs depending upon their formal constitution, or it may be a strategic service the offer to generally increase the level of data protection awareness and professionalism. |
| STAR Modules to use  (include key topics, and additional topics). | * Topic 1 – Introduction to the European Union Data Protection Regime (if required). * Topic 6 – the role of the data protection authority * Topic 4 – responsibilities of data controllers and processors * Topic 11 – It’s not just the GDPR – GDPR related laws and special provisions * Additional specialist topics, potentially including:   + Topic 7 - data protection in practice: Technical and organisational measures.   + Topic 8 - risk based approach in the GDPR   + Topic 9 - Data protection impact assessments   + Tropic 10 - Data protection communication |
| slides to use or remove |  |
| Supporting material to use | Intro to GDPR, compliance checklist, operational forms |
| how to specify for sector or national differences. | Replace private sector examples with public sector examples  Include references to foundational legislation for the entities being trained. |
| Further adaption needed from trainer / host | Pay particular attention to the legal grounds for processing personal data related to legal obligations.  Identify and include any transparency obligations for civil service  Identify and include any relevant national security exemptions |
| Additional reading | * Opinion 4/2007 of the Article 29 Data Protection Working Party of the European Commission on the concept of personal data (WP136) 20 June 2007 * Opinion 1/2010 of the Article 29 Data Protection Working Party on the concepts of controller and processor (WP169) 16 February 2010 * Handbook on European data protection law - 2018 edition <http://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law>   And see individual slide topics |
| Other comments |  |

|  |  |
| --- | --- |
| Scenario #4 – DPAs training judges | |
| Capsule description | The STAR slides are adapted by a data protection authority to provide specific training for judges. The aim here is bring judges up to speed on data protection issues. |
| Trainer | Data protection authority |
| Expected knowledge of Trainer | High |
| Trainee | Judges |
| Expected knowledge of Trainee | Very high legal knowledge, assumed working knowledge of data protection law and rapid ability to become familiar with the text, however, potentially limited practical experience of data protection. |
| Why use STAR? | To reduce the time and effort required for the trainer  To access and use the added-value elements of STAR based upon current research and academic thinking around data protection.  To improve harmonisation with training delivered at other DPAs (particularly important the likelihood of cross-jurisdiction data protection cases).  To allow quick responses to requests for support from judges. |
| Timing | 1 day |
| Delivery format | In person, potentially individually or small groups. |
| Self-directed or trained? | Trained |
| budgeting or other constraints | Staff-time cost, premises |
| Special considerations  (including pedagogic issues) | Expect this scenario to be very strongly led by the needs and interests of the trainee. It is worth identifying these before the training session is delivered. |
| STAR Modules to use  (include key topics, and additional topics). | * Topic 1 – Introduction to the European Union Data Protection Regime (if required) * Topic 6 – the role of the data protection authority * Topic 8 – Risk-based approach in the GDPR * Topic 7 – data protection in practice: Technical and organisational measures. |
| slides to use or remove |  |
| Supporting material to use | Intro to GDPR, operational forms |
| how to specify for sector or national differences. | Need to spend some time adapting the national slides to the relevant national context (these are marked within the training materials). |
| Further adaption needed from trainer / host | Topic 1 may not be necessary, or can be passed through at some speed if the trainee is already familiar with this material. |
| Additional reading | * Opinion 4/2007 of the Article 29 Data Protection Working Party of the European Commission on the concept of personal data (WP136) 20 June 2007 * Opinion 1/2010 of the Article 29 Data Protection Working Party on the concepts of controller and processor (WP169) 16 February 2010 * Handbook on European data protection law - 2018 edition <http://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law> * European Court of Human Rights, Press Unit (2018) *Factsheet – Personal Data Protection*, Council of Europe, Strasbourg; <http://echr.coe.int/Documents/FS_Data_ENG.pdf> * CJEU, C-275/06, Productores de Música de España (Promusicae) v. Telefónica de España SAU [GC], 2008 * ECtHR, Vereinigung bildender Künstler v. Austria, No. 68345/01, 2007 * CJEU, C-28/08 P, European Commission v. The Bavarian Lager Co. Ltd [GC], 2010 * CJEU, C-73/07, Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy [GC], 2008 * ECtHR, Axel Springer AG v. Germany [GC], No. 39954/08, 2012 * CJEU, C-101/01, Criminal proceedings against Bodil Lindqvist, 2003 * CJEU, C-582/14, Patrick Breyer v. Bundesrepublik Deutschland, 2016 |
| Other comments |  |

|  |  |
| --- | --- |
| Scenario #5 – DPA training (new) DPOs | |
| Capsule description | National supervisory authorities delivering classroom training sessions to newly appointed data protection officers. |
| Trainer | Data protection authority staff |
| Expected knowledge of Trainer | High (specialist) |
| Trainee | Data protection officer |
| Expected knowledge of Trainee | Moderate. May require some updating to GDPR issues. |
| Why use STAR? | To reduce the time and effort required for the trainer, and allow them to focus upon their organisational priorities.  To improve harmonisation with training delivered at other DPAs  To provide trainees with take-home material on other topics |
| Timing | Two days |
| Delivery format | Classroom |
| Self-directed or trained? | Trained |
| budgeting or other constraints | Staff-time cost, premises – can potentially be charged to the trainees, depending upon DPA constitution, obligations and strategy. |
| Special considerations  (including pedagogic issues) | The aim of training here is likely to establish a good common baseline standard for DPOs and to set clear expectations about their interaction and relationship with the data protection authority. |
| STAR Modules to use  (include key topics, and additional topics). | * Topic 1 – Introduction to the EU Data protection regime * Topic 2 – the rights of the data subject and their exercise * The rights of the data subject and their exercise. * Topic 4 – Responsibilities of data controllers and processors * Topic 5 – The role of the Data Protection Officer * Topic 6 – the role of the data protection authority |
| slides to use or remove |  |
| Supporting material to use | Intro to GDPR, compliance checklist, operational forms |
| how to specify for sector or national differences. | n/a |
| Further adaption needed from trainer / host | n/a |
| Additional reading | * WP29: Guidelines on Data Protection Officers <https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf>; * WP29 Guidelines on Data Protection Officers ANNEX - FREQUENTLY ASKED QUESTIONS, <https://www.alstonprivacy.com/wp-content/uploads/2016/12/2016-12-13-WP29-FAQs-on-DPOs-WP243-Annex.pdf> |
| Other comments |  |

|  |  |
| --- | --- |
| Scenario #6 – DPA training (experienced or established) DPOs | |
| Capsule description | National supervisory authorities delivering specialist classroom training session on specific topics to experienced data protection officers. |
| Trainer | Data protection authority domain expert |
| Expected knowledge of Trainer | High (domain expertise and experience in the topic chosen). |
| Trainee | Data Protection Officers |
| Expected knowledge of Trainee | Moderate to high. Interested in new developments in the GDPR and accessing/identifying best practice. |
| Why use STAR? | To reduce the time and effort required for the trainer, and allow them to focus upon their organisational priorities.  To improve harmonisation with training delivered at other DPAs  To benefit from the specialised focus of some of the later STAR materials. |
| Timing | Half-day |
| Delivery format | Classroom |
| Self-directed or trained? | Trained |
| budgeting or other constraints | Staff-time cost, premises – can potentially be charged to the trainees, depending upon DPA constitution, obligations and strategy. |
| Special considerations  (including pedagogic issues) | These sessions are likely deployed to spread best practice, and to conduct deeper dives into specific areas. Concrete examples are likely paramount. The trainer should be prepared to engage with concrete questions arising from the practical experiences of the trainees.  DPAs also gain the potential to understand issues and challenges that DPOs are facing in practice. |
| STAR Modules to use  (include key topics, and additional topics). | Uses a single module, as appropriate, from:   * Topic 7 – Data protection in practice: Technical and organisational measures * Topic 8 – Risk-based approach in the GDPR * Topic 9 – Data protection impact assessments * Topic 10 – Data protection communication * Topic 11 – It’s not just the GDPR - GDPR related laws and special provisions |
| slides to use or remove |  |
| Supporting material to use | Guidance on selected topic from the DPA,  Relevant Opinions on the selected topics from Article 29 Working party / EDPB. operational forms |
| how to specify for sector or national differences. | N/A |
| Further adaption needed from trainer / host | N/A |
| Additional reading | Please see individual slide topics |
| Other comments |  |

|  |  |
| --- | --- |
| Scenario #7 - DPA training for private sector (different sectors e.g. healthcare, education) | |
| Capsule description | In this scenario, the STAR training materials are used by a DPA to offer training for representatives of different industries and sectors. |
| Trainer | Data protection authority, Staff |
| Expected knowledge of Trainer | Expected to be very high - data protection professional, with some years of experience. |
| Trainee | Private sector DPOs |
| Expected knowledge of Trainee | Variable, may be first point of interaction with data protection, but may be professional specialists in other areas (e.g. management, HR). |
| Why use STAR? | To reduce the time and effort required for the trainer, and allow them to focus upon their organisational priorities.  To improve harmonisation with training delivered at other DPAs |
| Timing | 1 day |
| Delivery format | Classroom |
| Self-directed or trained? | Trained |
| budgeting or other constraints | Staff-time cost, premises – can potentially be charged to the trainees, depending upon DPA constitution, obligations and strategy. |
| Special considerations  (including pedagogic issues) |  |
| STAR Modules to use  (include key topics, and additional topics). | * Topic 1 – Introduction to the EU Data protection regime * Topic 2 – Purposes and legal grounds for data processing * Topic 3 – The rights of the data subject and their exercise * Topic 4 – Responsibilities of data controllers and processors |
| slides to use or remove | Add in slides from Topic 11 – It’s not just the GDPR – GDPR related laws and special provisions - that are relevant to the sector being trained. |
| Supporting material to use | Intro to GDPR, compliance checklist, operational forms |
| how to specify for sector or national differences. | If delivered for a particular industry or sector (e.g. education or healthcare), then this training needs the highest degree of specification from the base STAR materials. Examples can be shifted to apply directly to the industry of sector involved.  This specification should include prior discussion with industry representatives to identify the key issues facing that sector. |
| Further adaption needed from trainer / host | None |
| Additional reading | Please see individual slide topics |
| Other comments |  |

|  |  |
| --- | --- |
| Scenario #8 – Training to be published by a DPA for data controllers and processors | |
| Capsule description | Data protection authorities customise the training material to take into account their organisational priorities, branding and national specific legislation, then makes this available on their website, or by request, as guidance for data controllers and processors to use as required. |
| Trainer | DPA (to adapt material) |
| Expected knowledge of Trainer | High |
| Trainee | Data controller or processor (self) |
| Expected knowledge of Trainee | low |
| Why use STAR? | To provide freely available, good-quality training materials, developed with the support of EU DPAs.  To improve harmonisation with training delivered at other DPAs |
| Timing | One hour sessions, broken up over several weeks of real time, fitted around other workload commitments of the trainee |
| Delivery format | Online, downloaded PowerPoint slides |
| Self-directed or trained? | Self-directed |
| budgeting or other constraints | No budget/zero costs |
| Special considerations  (including pedagogic issues) | There is no trainer in this scenario.  Materials include notes on priority and importance to help guide.  Materials should be logically structured to help this user approach the material in the best order. |
| STAR Modules to use  (include key topics, and additional topics). | All (self-selected as required by the user, or taken in order)  High priority for:   * Topic 1 – Introduction to the EU Data protection regime * Topic 2 – Purposes and legal grounds for data processing * Topic 3 – The rights of the data subject and their exercise * Topic 4 – Responsibilities of data controllers and processors |
| slides to use or remove | No need to remove any slides |
| Supporting material to use | Intro to GDPR, compliance checklist |
| how to specify for sector or national differences. | N/A  However, this scenario would most likely benefit from the translation of STAR materials into common national languages. |
| Further adaption needed from trainer / host | None |
| Additional reading | Please see individual slide topics |
| Other comments |  |

# Training materials

## Presentations

Following D2.4 Training materials requirements, 11 Power Point presentations have been developed. The slides are meant to be easily adaptable to different audiences. To facilitate this, each slide is assigned to a specific audience (see „relevant for:” in the notes). In the notes-section below each slide useful information can be found (i.e. the trainer’s guidance):

* aim and objective of the slide,
* pedagogic strategies and guidance,
* timing (importance) of the slide,
* an indication of the slide’s degree of difficulty [i.e. whether it is suited for data protection beginners or not],
* its target audience [everyone vs authorities, lawyers, data protection officers, etc.],
* list of respective legal provisions,
* list of respective case law,
* list of respective additional reading,
* further notes,
* its degree of importance [whether it is essential to deliver it, or if it can be removed without impacting the effectiveness of the training].

However, the slides are not applicable immediately as they require customization and preparation. Prior to training delivery:

* the slides and the notes should be read thoroughly
* the reading materials should be considered as they also serve to assist the trainer in the preparation
* the slides that the trainer considers unnecessary should be removed/hidden [right click on the slide miniature on the left and click ‘hide slide’].
* slides should be adjusted to national or sectoral requirements
* content that the trainer considers essential for his or her particular audience should be added
* the default layout can be replaced with your other, more suitable (e.g. the organisation’s) layout

A provisional categorisation has been made based on the depth and importance of the respective content by using 4 different colours on the edges of the slides:

* Green – Is a basic slide: we encourage trainers to keep it
* Yellow – is a medium level slide: it is important, but does not jeopardise effectiveness if removed
* Red – is an advanced slide: adapting it to the trainer’s audience should be considered, trainer’s audience for it should be prepared, or, if it is deemed unnecessary, should be removed
* Purple – advised adaptation: this slide should contain information regarding the national legislation complementing the EU Regulations; if the content regards a different Member State, we advise trainers to replace it with the national, relevant content

The presentations will be continuously refined and updated based on the feedback and comments received by stakeholders.

**The presentations in .pptx format are available in the following link:**

<http://www.project-star.eu/training-materials>

## Reading materials

This section contains an indicative list of reading materials for each topic.

### Topic 1 – Introduction to the European Union Data Protection Regime

* **Required reading**
  + S Warren and L Brandeis, “The Right to Privacy” in Harvard Law Review. Vol. IV    December 15, 1890 No. 5 <http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html>
  + Handbook on European data protection law - 2018 edition <http://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law>
  + Opinion 4/2007 of the Article 29 Data Protection Working Party of the European Commission on the concept of personal data (WP136) 20 June 2007
  + Opinion 1/2010 of the Article 29 Data Protection Working Party on the concepts of controller and processor (WP169) 16 February 2010
* **Additional reading**
* Alan F Westin, Privacy and Freedom (New York Atheneum, 1967)
* Koops, B.-J. *et al.* (2016, ’A Typology of Privacy’ (2017) 38 University of Pennsylvania Journal of International Law 483) <https://scholarship.law.upenn.edu/jil/vol38/iss2/4/>
* Paul De Hert and Serge Gutwirth (2009) “Data protection in the case law of Strasbourg and Luxemburg: constitutionalisation in action” in: Gutwirth S., Y. Poullet, P. De Hert, J. Nouwt & C. De Terwangne (eds.) *Reinventing Data Protection?*, Springer, Dordrecht; <http://works.bepress.com/serge_gutwirth/10/>
* William L Prosser, ‘Privacy’ in California Law Review vol 48 issue 3 <https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=3157&context=californialawreview>
* **Case law**
* CJEU, C-101/01, Criminal proceedings against Bodil Lindqvist, 2003
* CJEU, C-275/06, Productores de Música de España (Promusicae) v. Telefónica de España SAU [GC], 2008
* CJEU, C-28/08 P, European Commission v. The Bavarian Lager Co. Ltd [GC], 2010
* CJEU, C-582/14, Patrick Breyer v. Bundesrepublik Deutschland, 2016

### Topic 2 - Purposes and legal grounds for processing personal data

* **Required reading**
  + Article 29 Working Party (2011), Opinion 15/2011 on the definition of consent, WP187, Brussels, 13 July 2011
  + Article 29 Working Party (2013), Opinion 3/2013 on purpose limitation, WP 203, 2 April 2013.
  + Article 29 Working Party, Opinion 2/2017 on data processing at work, WP 249, Brussels, 8 June 2017.
* **Additional reading**
  + Article 29 Working Party (2007), Working Document on the processing of personal data relating to health in electronic health records (EHR), WP 131, Brussels, 15 February 2007.
  + Article 29 Working Party (2014), Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 4 April 2014.
* **Case law**
  + ECtHR, Haralambie v. Romania, No. 21737/03, 27 October 2009
  + CJEU, Joined cases C-293/12 and C-594/12, Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others [GC], 8 April 2014
  + ECtHR, S. and Marper v. the United Kingdom [GC], Nos. 30562/04 and 30566/04, 4 December 2008.
  + CJEU, Joined cases C-293/12 and C-594/12, Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others [GC], 8 April 2014

### Topic 3 - The rights of the data subject and their exercise

* **Required reading**
  + Article 29 Working Party, Guidelines on Automated Individual Decision-Making and profiling for the purposes of Regulation 2016/679, WP 251, 3 October 2017
* **Additional reading**
  + Article 29 Working Party (2004), Opinion 10/2004 on More Harmonised Information Provisions, WP 100, Brussels, 25 November 2004.
  + Article 29 Working Party (2016), Guidelines on the right to data portability, WP 242, 13 December 2016 and revised on 5 April 2017
* **Case law**
* CJEU, C-131/12, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González [GC], 13 May 2014, paras. 55–58.
* CJEU, C-553/07, College van burgemeester en wethouders van Rotterdam v. M. E. E. Rijkeboer, 7 May 2009
* ECtHR, Cemalettin Canli v. Turkey, No. 22427/04, 18 November 2008, paras. 33 and 42–43;
* ECtHR, Ciubotaru v. Moldova, No. 27138/04, 27 April 2010, paras. 51 and 59

### Topic 4 - Responsibilities of data controllers and processors

* **Required reading**
  + Article 29 Data Protection Working Party Opinion 1/2010 on the concepts of "controller" and "processor
* **Additional reading**
  + OECD Privacy Guidelines 2013 - Accountability Principle: 14. A data controller should be accountable for complying with measures which give effect to the principles stated above.
  + Hielke Hijmans, „Principle of Data Protection: Renovation Needed?” Presentation to the International Data Protection Conference, Budapest, 2011
  + Art. 29 WP - Opinion 03/2010 on the principle of accountability (WP173)
* **Case law**

### Topic 5 – role of the DPO

* **Required reading**
  + WP29 Guidelines on Data Protection Officers Annex - Frequently Asked Questions <https://www.alstonprivacy.com/wp-content/uploads/2016/12/2016-12-13-WP29-FAQs-on-DPOs-WP243-Annex.pdf>
  + WP29: Guidelines on Data Protection Officers <https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf>;
* **Additional reading**
  + Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA
  + <https://gdpr-info.eu/issues/data-protection-officer/>
  + <https://www.insideprivacy.com/data-privacy/portuguese-hospital-receives-and-contests-400000-e-fine-for-gdpr-infringement>
  + <https://www.itgovernance.eu/blog/en/the-gdpr-what-is-sensitive-personal-data>
* **Case law**

### Topic 6 - Role of the DPA

* **Required reading**
  + WP29 Lead DPA Guidelines
* **Additional reading**
* **Case law**

### Topic 7 – technical and organizational measures

* **Required reading**
  + Article 29 Data Protection Working Party - Guidelines on Personal data breach notification under Regulation 2016/679 (WP250)
  + Article 29 Working Party Opinion 05/2014 on Anonymisation Techniques
* **Additional reading**
  + Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union
* **Case law**

### Topic 8: Risk-based approach to data protection

* **Required reading**
  + Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, 4 October 2017
  + Article 29 Data Protection Working Party, Statement on the role of a risk-based approach in data protection legal frameworks, 30 May 2014
  + European Data Protection Board, Opinions on the draft lists of the competent supervisory authorities regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR), 25 September2018
  + Information Commissioner's Office, Guide to the General Data Protection Regulation (2018)
* **Additional reading**
  + Centre for Information Policy Leadership at Hunton Andrews Kurth LLP (CIPL), Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR, 21 December 2016
  + Christopher Kuner et al., Risk Management in data protection, (2015) 5(2) International Data Privacy Law 95-98
  + Claudia Quelle, Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability- and Risk-based Approach, (2018) 9(3) European Journal of Risk Regulation 502-526
  + Raphael Gellert, Data protection: a risk regulation? Between the risk management of everything and the precautionary alternative, (2015) 5(1) International Data Privacy Law 3-19
* **Case law**

### Topic 9 - Data Protection Impact Assessments

* **Required reading**
  + Article 29 Data Protection working party Opinion WP248 rev01 Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679, October 2017
  + Kloza, D., Van Dijk, N., Gellert, R., Böröcz, I., Tanas, A., Mantovani, E., Quinn, P. (Brussels Laboratory for Data Protection & Privacy Impact Assessments (d.pia.lab)), Data protection impact assessments in the European Union: complementing the new legal framework towards a more robust protection of individuals - d.pia.lab Policy Brief No. 1/2017, 2017, ISSN 2565-9936 - <http://virthost.vub.ac.be/LSTS/dpialab/images/dpialabcontent/dpialab_pb2017-1_final.pdf>
* **Additional reading**
  + <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/>
  + David Wright and Paul De Hert (eds.), *Privacy Impact Assessment* (Springer, Dordrecht 2012)
* **Case law**

### Topic 10 - Data Protection Communication

* **Required reading**
  + The Article 29 Working Party guidance ( Guidelines on Automated individual decision-making and profiling for the purposes of Regulation 2016/679, WP251rev.01, 6 February 2018. - https://iapp.org/media/pdf/resource\_center/W29-auto-decision\_profiling\_02-2018.pdf
  + Article 29 WP251rev01. pg.26 - Full source available at: <https://iapp.org/media/pdf/resource_center/W29-auto-decision_profiling_02-2018.pdf>
  + Article 29 Working Party guidelines on automated individual decision making and Profiling for the purposes of Regulation 2016/679 –(WP251.rev1) http://ec.europa.eu/newsroom/article29/document.cfm?doc\_id=49826
* **Additional reading**
  + Guidance from Article 29 Working party on the Right to Portability https://ec.europa.eu/newsroom/article29/item-detail.cfm?item\_id=611233
  + The Royal Society, (2017), Machine Learning: the power and promise of computers that learn by example https://royalsociety.org/~/media/policy/projects/machine-learning/publications/machine-learning-report.pdf
  + Pasquale, Frank (2015), The Black Box Society: the secret algorithms that control money and information, Harvard University Press, Cambridge, MA.
  + Edwards, L. & Veale, M. (2017), Slave to the algorithm? Why a "right to explanation" is probably not the remedy that you are looking for. Duke Law and Technology Review. Available on SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract\_id=2972855
* **Case law**

### Topic 11 – It’s not just the GDPR - GDPR related laws and special provisions

* **Required reading**
  + Directive (EU) 2016/680 of the European Parliament and of the Council
* **Additional reading**
  + **Service sector**
    - Article 29 Working Party, Opinion 04/2012 on Cookie Consent Exemption
    - Article 29 Working Party, Working Document 02/2013 providing guidance on obtaining consent for cookies
    - Data protection self-assessment : <https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/>
    - Directive 2011/83/EU of the European Parliament and of the Council
  + **Employment**
    - Article 29 Working Party, Opinion 2/2017 on data processing at work, Adopted on 8 June 2017.
    - De Hert Paul, Lammerant Hans (2013) Protection of personal data in work-related relations. Study made on behalf of the European Parliament's Committee on Civil Liberties, Justice and Home Affairs. European Parliament.
  + **Education and science**
    - Convention on the Rights of the Child <https://www.ohchr.org/en/professionalinterest/pages/crc.aspx>
    - What is important for Data Protection in science in the future? <https://www.ratswd.de/dl/RatSWD_WP_258.pdf>
  + **Healthcare**
    - Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR) (art. 70.1.b)) <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinionctrq_a_final_en.pdf>
    - Citizen-Controlled Data Governance and Data Donors” Opportunities & risks for consumers
    - <https://www.eiseverywhere.com/file_uploads/bdb85215fdd938aa672694c2a765529d_francesca-cattarin_Citizen-Controlled-Data-Governance-and-Data-Donors.pdf>
    - EDPS Decision concerning the transfers of personal data carried out by the European Centre for Disease Control to the World Health Organisation pursuant to Article 9(7) of Regulation (EC) No 45/2001 <https://edps.europa.eu/sites/edp/files/publication/18-01-17_annex_2017-1120_en.pdf>
* **Case law**

## Operational forms

### Attendance sheet

The attendance sheet is available in the following link:

<http://www.project-star.eu/training-materials>

Please note that the style of the document might have changed because of the deliverable format. The content remained unchanged. For the original document please visit the website.

|  |
| --- |
| **STAR GDPR training sign in sheet** |

|  |  |  |  |
| --- | --- | --- | --- |
| **Training Course** |  | **Meeting Date:** |  |
| **Facilitator:** |  | **Place/Room:** |  |

| **Name** | **Organisation** | **E-Mail** | **Signature** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |



### Evaluation questionnaire

The evaluation questionnaire is available in the following link:

<http://www.project-star.eu/training-materials>

Please note that the style of the document might have changed because of the deliverable format. The content remained unchanged. For the original document please visit the website.

****  
**STAR  
Support Training Activities on the data protection Reform  
project-star.eu**

**TRAINING EVALUATION QUESTIONNAIRE**

[Topic] – [Location/Organisation]

[Date]

**Please give us your overall opinion on the course**. (0 = very bad; 4 = excellent)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | 0 | 1 | 2 | 3 | 4 |
| 1. The objectives of the training were clearly outlined |  |  |  |  |  |
| 2. The presentation was engaging |  |  |  |  |  |
| 3. The presentation materials were relevant |  |  |  |  |  |
| 4. The content of the course was organised and easy to follow |  |  |  |  |  |
| 5. The trainers were well prepared and able to answer any questions |  |  |  |  |  |
| 6. The course length was appropriate |  |  |  |  |  |
| 7. The pace of the course was appropriate to the content and attendees |  |  |  |  |  |
| 8. The exercises/role play were helpful and relevant |  |  |  |  |  |
| 9. The venue was appropriate for the event |  |  |  |  |  |

**More specifically on the training materials**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | 0 | 1 | 2 | 3 | 4 |
| 1. The training materials’ design met my expectation |  |  |  |  |  |
| 2. The amount of information contained in the presentation was adequate |  |  |  |  |  |
| 3. The language in the materials was adequate to my level of knowledge |  |  |  |  |  |
| 4. The materials would be useful for future reference |  |  |  |  |  |
| 5. I would be able to rearrange / reuse these materials easily |  |  |  |  |  |

**What was most useful?**

|  |
| --- |
|  |

**What was least useful?**

|  |
| --- |
|  |

**Any other comments**

|  |
| --- |
|  |

## Compliance checklist

The compliance checklist is available in the following link:

<http://www.project-star.eu/training-materials>

Please note that the style of the document might have changed because of the deliverable format. The content remained unchanged. For the original document please visit the website.

GDPR compliance checklist

Use this checklist to help your organization achieve compliance with the requirements of the General Data Protection Regulation (GDPR)

Homework Tips Checklist for Parents

# Does the GDPR apply to you?

Are you processing personal data?

Are you established in the EU or are you processing personal data of people resident in the EU?

If you ticked both of these, then the GDPR applies to your organization.

# Know what data you have or intend to process

Conduct an information audit to map the data you hold, its sources, who you share it with, and what you do with it.

Document your purposes for processing personal data

Determine if you are processing any special categories of data (e.g. children's personal data, sensitive personal data).

Identify and document the legal basis for the personal data you hold.

Determine how long you need to retain this data.

Decide who needs access to this data, and how you can restrict access to it (for example, by role-based access, or segregation of duties).

Document any processor or sub-processors (anybody which processes personal data on your behalf) you use, and what data they hold. Have a contract with each processor. Do due diligence with regard to your processors.

Determine if you are transferring personal data outside the EU and if so, that adequate protections are in place.

Review and audit the data you hold on a regular basis.

# Conduct a data protection impact assessment

Determine if any of the data processing is high-risk to the rights of data subjects[[1]](#footnote-2) or on the list of processing activities that require a data protection impact assessment produced by national supervisory authorities.[[2]](#footnote-3)

Conduct a data protection impact assessment[[3]](#footnote-4), including an assessment of the risks to the rights and freedoms of data subjects.

If you identify serious risks, that cannot be mitigated, then consult with the supervisory authority BEFORE commencing data processing.

Conduct DPIA for new programs, systems and processes.

# Establish organisational process

Decide leadership responsibility for data protection

Appoint a data protection officer, if necessary or recommended[[4]](#footnote-5)

Establish, keep up to date and test technical information security measures.

Decide how you will respond to a subject access request

Decide how you will respond to a request for data erasure, rectification, restriction of processing, or request for data portability, or withdrawal of consent

Train staff on their data protection responsibilities[[5]](#footnote-6)

Establish a protocol for identifying and reporting breaches of personal data security

Integrate data protection into any direct marketing practices

Integrate data protection into records retention practices.

# Communication and Accountability

Identify any approved codes of conduct that apply to your data processing

Draft and publish a clear, understandable privacy policy

Explain to data subjects how and why you need their data at the point of collection.

Ask for consent clearly and separately from other terms and conditions

Explain how and why profiling or automated decision making is used.

Establish and maintain a data protection incidents log

Record processing activities and be able to provide this to a supervisory authority on request.

Ensure regular communication between DPO and others responsible for data protection

# Get assistance and support

Identify useful sources of guidance from your national data protection supervisory authority

Check other GDPR guides, resources and training available at www.project-star.eu

This guide was produced by the STAR project (*Support Training Activities on the data protection Reform*; 2017-2019), which is co-funded by the European Union under the Rights, Equality and Citizenship Programme 2014-2020 (REC-RDAT-TRAI-AG-2016) under Grant Agreement No. 769138.

More information, and other GDPR training resources can be found at: **www.project-star.eu**



## Introductory guide to the GDPR

The introductory guide is available in the following link:

<http://www.project-star.eu/training-materials>

Please note that the style of the document might have changed because of the deliverable format. The content remained unchanged. For the original document please visit the website.

A one-page guide to the General Data Protection Regulation (GDPR)

I've heard about this "GDPR", but what is it?

Formally, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of personal data wand on the free movement of such data, and repealing Directive 95/64/EC (General Data Protection Regulation), but most often shorted to "the GDPR"

It was adopted in 2016 and came into effect in May 2018.

You can find a full copy of the legislation in all EU official languages at <http://data.europa.eu/eli/reg/2016/679/oj>

The GDPR applies to data controllers established in the EU, and to personal data of people in the EU, even if processed by a controller not established in the EU. It does not apply to household or purely personal use of personal data.

The purpose of the GDPR is to update and modernise laws that **protect the personal information of individuals**, and to provide an equal level of protection across the EU.

**Personal data** is any information relating to an identified or identifiable natural person. This is a wide and inclusive definition. There are also some categories of *sensitive* personal data (such as racial or ethnic origin, political or religious beliefs, health data) that get extra protection because abuse of personal data in these categories is likely to lead to harmful consequences. Processing of personal data is any activity performed on personal data (such as collecting, storing or organising it).

The GDPR is based around **principles of lawfulness, fairness and transparency; purpose limitation; data minimisation, accuracy; storage limitation; integrity and confidentiality, and accountability**. To process personal data, an organisation (a "data controller") must have clear purposes and a legitimate ground for doing so. The data must be kept for no longer than necessary, must be accurate and up to date. The controller must also take measure to ensure the data is processed properly and securely. The principle of accountability means that organisations processing personal data are responsible for demonstrating that they are doing so in lawful, fair and transparent.

The GDPR grants people many **rights**. When their data is processed, they must be provided with contact details for the data controller, information on the purposes of processing, how long the data will be stored, if they are obliged to provide data, sources of data, if the data will be transferred to third parties, information about any automated decision making and information about their other data protection rights. These include rights to request access to, correction or erasure of personal data, restriction of processing, to object to processing and to receive their data in a portable form. They also have the right to lodge a complaint about data processing with a supervisory body.

If you have any further questions, or think you need further training on the GDPR, then please contact our Data Protection Officer:

Name: [user to complete]

Email: [name@organisation.com](mailto:name@organisation.com)

Phone: [user to complete]

This guide was produced by the STAR project(*Support Training Activities on the data protection Reform*; 2017-2019), which is co-funded by the European Union under the Rights, Equality and Citizenship Programme 2014-2020 (REC-RDAT-TRAI-AG-2016) under Grant Agreement No. 769138.

More information, and other GDPR training resources can be found at: **www.project-star.eu**



To protect those rights, the GDPR empowers independent supervisory bodies (sometimes also called **Data Protection Authorities** or Information Commissioners) to oversee compliance with the GDPR and to promote awareness of GDPR obligations and rights. These bodies work together as the European Data Protection Board.

The GDPR also introduces significant **penalties** for non-compliance. Supervisory bodies can carry out investigations, issue warnings and reprimands to controllers, and impose fines up to €20 million or 4% of worldwide turnover for serious infringements of the GDPR.

1. Likely when processing involves new technologies; When no DPIA has been done before; Long time since initial processing; Large scale processing operations; Considerable personal data; Regional, national or supranational level; Affect a large number of data subjects; New technology used at large scale; Taking decisions about natural persons based on systematic or extensive evaluation of personal aspects (profiling;

   Processing special categories, biometric data, data on criminal convictions; Monitoring publicly accessible areas on large scale; where processing might prevent people exercising a right or using a service/contract; or any operations where a supervisory authority considers that processing is likely to result in high risks [↑](#footnote-ref-2)
2. The European Data Protection Board has commented upon each of the draft lists of competent supervisory authorities of processing operations that require a data protection impact assessment: https://edpb.europa.eu/our-work-tools/consistency-findings/opinions\_en [↑](#footnote-ref-3)
3. See the Article 29 Working party Opinion WP268 on data protection impact assessment: https://ec.europa.eu/newsroom/document.cfm?doc\_id=47711 [↑](#footnote-ref-4)
4. <https://trilateralresearch.co.uk/these-six-organisations-are-considering-appointing-a-dpo-and-yours/> [↑](#footnote-ref-5)
5. The STAR project has created downloadable GDPR training materials for a variety of purposes, including training staff in their data protection obligations. These materials are available free of charge from [www.project-star.eu](http://www.project-star.eu) [↑](#footnote-ref-6)