STAR

SUPPORT TRAINING ACTIVITIES ON THE DATA PROTECTION REFORM

PROJECT-STAR.EU

HANDBOOK FOR SUPPORTING TRAINING ACTIVITIES ON THE DATA PROTECTION REFORM

István Böröcz
Paul De Hert
David Barnard-Wills
Filippo Marchetti
Gábor Kulitsán
Renáta Nagy
Júlia Sziklay

Brussels – London – Budapest
October 2019

Prepared for the European Commission's Directorate-General for Justice and Consumers (DG JUST).

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

Institutional Members of the STAR Consortium	
Member	**Role**
Vrije Universiteit Brussel (VUB), Research Group on Law, Science, Technology and Society (LSTS)	Project Coordinator
Trilateral Research Ltd. (TRI)	Partner
Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH)	Partner

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.

Permanent link: http://www.project-star.eu/handbook

version 1.0
15 October2019

Disclaimer

The contents of this handbook are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission. Neither the European Union institutions and bodies nor any person acting on their behalf may be held responsible for the use which may be made of the information contained therein.

Foreword

The STAR project (Support Training Activities on the data protection Reform) aimed to contribute to a more effective application of the EU data protection reform package, through handing out to two categories of trainers (data protection authorities and data protection officers) ready-made and easily customizable training materials necessary to carry out their training operations. With such materials, trainers can reduce their workload, as the ground-setting work has already been carried out for them by STAR. In order to further assist their training activities, the STAR consortium provides trainers with this handbook, facilitating an efficient organization of data protection-oriented training and, use of the STAR training materials.

The handbook is a result of the commitment and hard work of the STAR consortium partners, István Böröcz and Paul De Hert from the Vrije Universiteit Brussel; David Barnard-Wills and Filippo Marchetti from Trilateral Research Ltd.; and Júlia Sziklay, Gábor Kulitsán and Renáta Nagy from the Hungarian National Authority for Data Protection and Freedom of Information.

They based their work not only on the respective EU legal framework and academic literature, but engaged with stakeholders multiple times throughout the project, assessed their actual needs, and changed the outputs according to their views, ensuring that present handbook and the respective materials will truly assist trainers in their work.

The STAR handbook aims to assist trainers in delivering training on the General Data Protection Regulation (GDPR), and in particular those trainers making use of the STAR training materials. Whilst each of the STAR training materials include individual guidance, this handbook provides guidance and support across the range of materials.

This handbook does not contain all the factual content of the GDPR, as those reside in the training materials, but serves as a complementary tool thereto. To facilitate its editing and re-use within organisational environments, the handbook is provided in a .doc format, besides the formatted .pdf version.

***István Böröcz**, Vrije Universiteit Brussel (VUB)*
***Paul De Hert,** Vrije Universiteit Brussel (VUB)*
***David Barnard-Wills**, Trilateral Research Ltd. (TRI)*
***Filippo Marchetti**, Trilateral Research Ltd. (TRI)*
***Júlia Sziklay**, Hungarian National Authority for Data Protection and Freedom of Information (NAIH)*
***Gábor Kulitsán**, Hungarian National Authority for Data Protection and Freedom of Information (NAIH)*
***Renáta Nagy**, Hungarian National Authority for Data Protection and Freedom of Information (NAIH)*

Contents

Introduction

In 2009, with the Lisbon Treaty and the Charter of Fundamental Rights of the European Union, the EU has given a reinforced emphasis on data protection as a fundamental right. Respectively, the 95/46/EC Data Protection Directive became technologically outdated over the years, thus in the same year the European Commission started a public consultation regarding the amendment of the Data Protection Directive. The Directive was then almost 15 years old, and one of the main concerns was the insufficient level of harmonisation between Member States. The consultation was followed by a lengthy reform process, which concluded in April 2016. The data protection reform, comprising essentially of the General Data Protection Regulation (Regulation 2016/679; GDPR) and the Police and Criminal Justice Data Protection Directive (Directive 2016/680; Directive) is one of the pivotal building blocks of a Connected Digital Single Market and an Area of Justice and Fundamental rights based on Mutual Trust. The GDPR is expected to solve harmonisation problems, caused by the 95/46/EC Data Protection Directive, as it is directly applicable. This enhances the effectiveness of the framework, not to mention the qualitative change it evokes: to underline its importance, data protection moved to EU level from the level of Member States. As Recital (9) GDPR underlines: *„Directive 95/46/EC… has not prevented fragmentation in the way data protection is implemented across the Union, legal uncertainty and a widespread public perception that there are significant risks for the protection of individuals..."*

To achieve its goal, the data protection reform package has to be effectively implemented, monitored and, most importantly, applied by Member States, in particular by data protection authorities (DPAs) as well as other public authorities, legal professions such as members of the judiciary and lawyers as well as data protection officers (DPOs).

Consequentially, EU DPAs and DPOs have to adapt to the new regulatory environment. They need to follow closely their respective Member State's national legislation both giving full effect the GDPR and transposing the Directive; they need to release their own guidelines for their respective jurisdictions and adapt their routine practices; they need to participate in EU work on applying the new framework. All of the above, on top of their routine, day-to-day data protection work put a vast new burden on DPAs' and DPOs' day-to-day routine. Furthermore, the GDPR requires these two categories of data protection actors to undertake training activities (according to Art. 57(1) and 39(1)(b) GDPR) in order to assist stakeholders (i.e. those groups who are affected by the GDPR) in the adaptation process. Training is defined as a planned, systematic effort to modify or develop knowledge, skill or attitude through learning experiences, to achieve effective performance in an activity or range of activities. The purpose of this activity in professional situations is to enable the trainee to acquire abilities for the adequate performance of a given task or job. Training materials are those supporting texts, presentations, guides, manuals, and other physical and digital materials that are used in or for those systematic efforts.

The training requirements are also expected to be contextualised against one of the policy intents behind the GDPR – increasing legal certainty and providing a level playing field for data controller. Effectively, harmonisation of data protection regulation across the EU. Each DPA and DPO developing training programmes and materials in isolation increases the overall cost involved, risks undermining the harmonising effect of the GDPR, spreading different sets of competing interpretations and best practices and puts greater pressure on the GDPR consistency mechanisms. The financial and human resources (including staff numbers) of EU DPAs and DPOs are also highly variable, meaning that not all have the

capacity to generate training materials efficiently. Common training programmes would be both an example of increased coordination between data protection authorities, and an aid to this coordination.

The *STAR project (Support Training Activities on the data protection Reform)* aimed to address these burdens in cooperation with the stakeholders and provide support to the training activities of European Union data protection authorities and data protection officers on the EU data protection reform, especially the General Data Protection Regulation. These ready-made, easy-to-customise and easy-to-run training materials are easily adaptable to specific training situations and they are freely and publicly available in a digital form, saving thus time and reducing the workload of trainers and facilitating a harmonized training of the GDPR across the EU.

The aim of the training materials is to significantly reduce the overheads and difficulties of assembling and delivering GDPR training sessions by domain experts, not to replace these experts. Respectively, as experts, the users of the training materials can and should modify these materials. STAR cannot anticipate all situations, but it is aiming for wide-as-possible coverage and usability and provides guidance thereto. The STAR training materials encompass the diversity of various levels of experience, from no previous knowledge of the GDPR, to experienced data protection professionals looking for practical strategies.

THE TRAINING MATERIALS INCLUDE:

- 11 TRAINING TOPICS FOCUSING ON THE GDPR
- SEMINAR MATERIALS (I.E. MICROSOFT POWERPOINT PRESENTATIONS) FOR EACH ONE OF THE TOPICS WITH DETAILED GUIDANCE FOR TRAINERS AND SUGGESTED READING MATERIALS
- TRAINING SCENARIOS
- A TAKEAWAY REFERENCE GDPR CHECKLIST
- A TEN-POINT GDPR INTRODUCTORY LIST
- AN EVALUATION QUESTIONNAIRE FOR ATTENDEES

This handbook serves as a guiding document for DPAs and DPOs on how to use these materials. It provides trainers with additional knowledge around GDPR training that has been gathered by the STAR consortium, including feedback gathered through stakeholder interviews and trials of the STAR materials. The handbook sensitises trainers to issues that may emerge in GDPR training and provides pedagogic support to trainers who may lack previous training experience (e.g. a DPO).

The handbook is not intended to contain all the factual content on the GDPR, this resides in the seminar material for each of the topics (e.g. in Microsoft PowerPoint presentations).

The structure of this book is the following: Section 1 elaborates on the challenges in GDPR training, based on the feedback gathered from interviewees (DPAs and DPOs). The second section highlights a selected list of best practices in GDPR training and defines what a “good” GDPR training should comprise. Section 3 provides selected questions and answers from trainings to assist the trainer in the preparation for Q&A sessions. Section 4 describes how the training materials should be used by the trainer. Section 5 provides a set of training scenarios where the STAR training materials could be used. Finally, Section 6 assists trainers to adapt the STAR training materials to their specific needs.

creation. This is the most accommodating of the Creative Commons licenses. It is recommended for maximum dissemination and use of licensed materials. The terms of this license are available at:

- https://creativecommons.org/licenses/by/4.0/ and
- https://creativecommons.org/licenses/by/4.0/legalcode

1. Challenges in GDPR training

No training should be considered easy. Each subject, domain or skill has its own oddities, and places different requirements upon the learner and the trainers supporting them. Through our own training experiences and the process of scoping the STAR training materials, we have identified a set of challenges that apply to the field of GDPR training:

- **Correcting myths and misconceptions -** In the run up to the GDPR coming into force, there was room for many myths and misconceptions to come into existence and gain credibility. This has not been helped by some organisations using "The GDPR" as cover for other anti-competitive, or anti-transparency practices. Since the GDPR has come into force, people will have come into contact with it, or changes introduced in response to it, in a range of contexts - some of them handled better than others! This means that any GDPR training has to deal with existing myths and misconceptions about the GDPR and its requirements amongst the trainees.
- **Diversity of trainees -** Given the prominence of data processing in modern society and economies, the GDPR is a regulatory regime that touches on a great many areas of modern life. As a result, individuals and organisations requiring training on data protection law can come from an extremely broad range of backgrounds, bringing with them particular ways of working, organisational cultures, levels of technical and technological knowledge and capacity. This is a challenge for a trainer because they likely need to know something about these backgrounds, and in particular the different needs of the trainee.
- **GDPR intersection with other legal regimes** - the GDPR does not exist in isolation and many potential trainees will want to understand how the GDPR interacts with other regulatory regimes that impact upon them - for example, how do the rights of the data subject interact with obligations on organisations to retain records for oversight and accountability purposes? Even in the world of data protection, we found that existing training material rarely encompasses the other data protection regulations in force, such as Directive 2002/58/EC (ePrivacy Directive).
- **Different training needs between data protection authorities and data protection officers** - On the one hand, authorities tend to deliver (and consider most important to deliver) more institutional, theoretical training on the GDPR, aimed at creating in trainees a clear picture of the legal framework in which both regulat*ors* and regulat*ed* operate. On the other hand, other stakeholder trainers, in particular those who provide training for a profit, tend to focus on more operative aspects, such as procedures and methods to comply with the GDPR provisions.
- **Demand -** There is significant demand for GDPR training, however, there is relatively little engagement with alternative methods of training provision.
- **No certification for trainers** - despite the opportunity for certification present in the GDPR (article 42) there is, as yet, no certification available to ensure that a trainer offering training on the GDPR has sufficient knowledge and experience to provide that training. This means that training can be of mixed quality, and that there is some caution on the part of the potential trainees and customers of training.
- **The authority of the regulator -** Many potential trainees (as well as trainers) want to know what the perspective of the regulatory authorities is. They understand that training should be based upon how their conduct will (potentially) be regulated, and see DPAs as the authoritative source in this domain. Whilst many EU data protection authorities are producing guidance material (see below) others are still waiting on national legislation, and not all EU DPAs see providing training as being their responsibility, and the external training some provide is not strategic.
- **Lots of "training" is actually just something to read** - for example, most DPAs have developed informative materials and made them available on their websites to ensure that organisations and

citizens in need of information on the GDPR innovations may access knowledge for free and from an official source. However, these materials are mostly means for passive dissemination, such as handbooks and info-sheets, or sometimes videos. When we looked at available training materials, what was often missing was any discussion of the methodology of *how* the training should be conducted.

2. Best practices in GDPR training

Based upon the interview and documentary research conducted in the STAR project,[1] we offer a checklist of what we consider to be good practices in GDPR training. In this section our aim is threefold. This checklist outlines the principles behind the STAR GDPR training material - we developed the STAR materials to meet all these requirements. We hope that this checklist provides other people or organisations designing or delivering GDPR training with guidance on how best to develop their training.

We also hope that this checklist provides those looking for data protection training in this new regulatory context a guide with which they can evaluate what is being offered to them or is available on the market.

A "good" GDPR training:

- **Covers (at minimum) the following topics:**
  - Introduction to the EU GDPR regime
  - Purposes and legal grounds for processing personal data
  - The rights of the data subject and their exercise
  - Responsibilities of data controllers and processors
  - The role of the Data Protection Officer
  - The role of the Data Protection Authority
  - Data protection in practice (including technical and organisational measures)
  - Risk management in the GDPR context.
  - Data Protection Impact Assessments
  - Data protection communication
  - GDPR-related laws and special provisions
- **Is clear about its target audience, or specifically adapted to its target audience and its particular training needs** - a potential customer of GDPR training should try to understand their particular training needs and select training resources appropriately. GDPR training can be particularly useful if it is designed for use within a particular context or sector, focusing upon common occurrences and practices in that sector, for example, data protection in medical, banking finance, education, marketing industries, or in the law enforcement context.
- **Is orientated towards longer term use** – training should be designed for longer term use and not overly focus upon what is "new" in the GDPR, but rather on what is important, complex or otherwise requires training material. This becomes more pertinent over time as fewer data protection professionals will have pre-GDPR experience.
- **Is customisable -** ready for localisation to enable DPAs/DPOs to amend as required (for example, for them to add own logos and trademarks, but also institutional design languages – e.g. corporate colours and fonts) and otherwise interact with as they wish.
- **Is easily understandable by its target audience** - It should avoid the use of legal jargon where possible, and explain any necessary specialised terminology; define key concepts and terminology; and make good use of graphical elements to support written text.

[1] In the project the consortium carried out qualitative interviews in January-April 2018 with representatives of the Member States' DPAs and public and private sectors' DPOs. These interviews aimed to identify the current training practices of both categories of stakeholders and assess their foreseeable needs for the future. The second source of information is a collection of existing training materials that the research consortium obtained from the interviewees and by carrying out extensive research on the DPA websites, as well as on the websites of other organisations that provide GDPR.

- **Includes practical examples and case studies** - as these were demanded by GDPR stakeholders and their use is supported by educational theory.[2] Such cases can include synthetic case studies, generated to highlight specific issues or teaching points, but real case studies are particularly desired. Case studies promote vicarious experience for learners.
- **Meets commonly used accessibility standards -** the assessment of existing GDPR training material from various sources, conducted here found that very little of this material meets current accessibility best practices. Users should not be prevented from accessing GDPR training because of visual or other disabilities.
- **Provides practical guidance and instructions -** for example, how-to instructions, Frequently-Asked-Questions lists, to-do lists, best practices, templates and tools.
- **Is interactive** - practical exercises for trainees should be included where possible. interactive sessions, facilitate and encourage discussion and interaction between participants. Interaction was strongly identified by stakeholders as a key source of learning and sharing of experience.
- **Is delivered by a subject-matter expert** – whilst introductory training can be delivered by generalist trainers, much GDPR training for specialists in practices involves exploring particular questions, examples and edge-cases and in this, domain expertise and the ability to go beyond the text of training materials remains critical.

[2] Clark, Ruth, "Accelerating Expertise with Scenario-based learning", Training and Development, January 2009. http://www.clarktraining.com/content/articles/ScenarioBasedLearning.pdf

3. F.A.Q from GDPR training

NAIH staff often participate at training courses, lectures and conferences providing information on GDPR compliance. Audiences usually ask both theoretical and practical questions. Theoretical questions focus on clarifying the basic concepts of data protection law, while practical ones cover data protection impact assessments, data breaches, possible penalties and fines, and the obligation to designate a DPO. Audiences are also much interested in the lawfulness of concrete instances of data processing: does a specific data processing comply with the GDPR, would there a best practice available, what should be done differently, etc. The issues of the legal basis of the data processing and the need for conducting a legitimate interest assessment also often emerge during training courses.

3.1 FAQs addressed to DPAs

1. Maintaining a record of processing activities

How can I notify the data processing I carry out to the data protection authority?

The GDPR does not provide for a national data protection register to be maintained by the authorities of Member States. Article 30 of the GDPR obligates each data controller, and data processor, to maintain a record of processing activities under its responsibility. This means that the data controllers, and data processors, themselves must maintain records of their data processing activities without having to notify the Authority thereof. The obligation to notify data processing to the data protection register ceased as of 25 May 2018.

Must a data processor also maintain a data processing record?

Yes. Article 30 (2) of the GDPR defines the content of such a record. Accordingly, each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller. Pursuant to Article 30 (3) of the GDPR, such a record shall be in writing, including in electronic form.

Does the GDPR provide for any exemption in view of SMEs?

Article 30 (5) of the GDPR exempts enterprises employing less than 250 persons from the obligation to maintain a record unless the processing they carry out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data.

2. Designation of a DPO

As an SME, how am I to assess whether I am obliged to designate a DPO or not?

Article 37 (1) defines the cases when a data protection officer must be designated.

With respect to SMEs, it is Article 37 (1) b) that is governing, pursuant to which a data protection officer shall be designated where ‘the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale’ The notification shall include the names of the data

controller and data processor, their contact details, the name, postal and electronic address of the data protection officer.

3. Data breach

How should I notify the supervisory authority in case of a data breach?

1. The data controller shall maintain a record of data breaches, indicating the facts related to the data breach (scope of data subjects and personal data, the time and circumstances of the breach), its effects, and the measures taken to remedy it.

2. The data controller shall, without undue delay but not later than within seventy-two hours after having become aware of it, notify the personal data breach to the Authority, except when it is unlikely to result in a risk to the enforcement of the data subjects' rights.

3. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without delay.

Does the data controller have any obligation other than notifying the Authority when a data breach occurs?

Yes. First, it has to maintain record of data breaches, indicating the facts of the breach, its effects, and the measures taken to redress it. Second, if the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without delay, indicating:

- the name and contact details of the data protection officer or other contact point;
- the likely consequences of the breach;
- the measures taken or proposed to be taken by the data controller.

What must the data breach notification include?

As minimum, it must:

- describe the nature of the personal data breach, including, where possible, the scope and approximate number of data subjects concerned, as well as the scope and approximate number of personal data records concerned,
- communicate the name and contact details of the data protection officer or other contact point designated to provide more information,
- describe the likely consequences of the personal data breach, and
- describe the measures taken or proposed to be taken by the controller.

What is to be done when not all the circumstances of the data breach are known, or do not become known until the expiry of the 72-hour deadline under Article 33 of the GDPR?

If information cannot be communicated at once, they can be communicated in parts without undue further delay.

4. Sanctions

If the processing of data does not comply with the GDPR, what penalty should I expect as an SME?

Article 58 (2) of the GDPR defines the corrective measures the Authority may apply in the event of an infringement of data protection rules, one of which is the imposition of administrative fines.

Article 83 of the GDPR lays down the general conditions for imposing administrative fines. According to Article 83 (1) the imposition of administrative fines shall in each individual case be effective, proportionate and dissuasive. According to Recital (148), in a case of a minor infringement or if the fine likely to be imposed would constitute a disproportionate burden to a natural person, a reprimand may be issued instead of a fine.

Infringements of Article 83 (4) of the GDPR shall be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher. Infringements of Article 83 (5) shall be subject to an administrative fine of up to EUR 20 million or up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher. The latter includes, inter alia, violations of the principles of data processing (Articles 5–7, 9 GDPR), including the conditions of consent and violations of the rights of data subjects (Articles 12–22 GDPR).

5. Rights of the data subject

In case maintaining a record of data transfers is necessary, is it sufficient to provide information to clients and employees on the categories of data, the recipients and the legal basis of the data transfer in the data protection notice?

Article 12 of the GDPR details the obligations of the controller with respect to the mode information to be provided concerning data processing. On this basis, 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, using clear and plain language.

Articles 13 or 14 of the GDPR define the information to be provided to the data subject (depending on whether the personal data relating to the data subject is collected from the data subject or from another person/organisation respectively):

(a) the identity and the contact details of the controller and, where applicable, of the controller's representative;

(b) the contact details of the data protection officer, where applicable;

(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

(d) where the processing is based on point (f) of Article 6 (1), the legitimate interests pursued by the controller or by a third party;

(e) the recipients or categories of recipients of the personal data, if any;

(f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

Points (e) and (f) of paragraphs (1) in both Articles 13 and 14 state that the controller is required to inform the data subjects on the recipients or categories of recipients of the personal data when personal data are communicated (e.g. by transfer), furthermore in case the controller intends to transfer personal data to a recipient in a third country or international organisation on the details of such transfer, i.e. the same information must be provided to the data subject as the controller is obliged to keep record of.

Accordingly, practice in compliance with the Regulation is when the controller provides information on the categories of the data transmitted, recipients and the legal basis of the data transfer to the data subject in a written notice, with the proviso that the data controller shall provide information on all the details of data processing (including data transfer) in the event of a data access request by the data subject in under Article 15 of the GDPR.

3.2 FAQs addressed to DPOs

1. Data of employee's

Under what conditions may employees process the certificates of good conduct of employees?

In the opinion of the Authority based on the relevant provisions of the GDPR and the Privacy Act, employers may process the personal data of their employees concerning criminal actions, the related security measures, and their having no criminal record, first, on the basis of Article 6 (1) c) of the GDPR (processing is necessary for compliance with a legal obligation to which the controller is subject) and, second, based on the authorisation of an Act detailing the processing.

Note, however, employers may only require their employees to show them their certificates of good conduct; they may not make copies of them.

May an enterprise use GPS in its company cars?

An indispensable condition of lawful data processing is that data processing has a legal basis under Article 6 of the GDPR; according to Article 6 (1) f), data processing may be lawful when it is necessary for the purposes of the legitimate interests pursued by the controller.

If the employer has also a legitimate interest in using tracking system, the first issue to be examined is whether the data processing is by all means necessary for the purposes designated by the employer, and whether its implementation by a GPS device is proportionate to the limitation on rights.

It is particularly important that employers inform their employees of installing tracking devices in the company cars their employees drive, and that while they use the vehicle, their movements are recorded.

It is adjudged differently when employees may also use company cars for private purposes; in this case, there can be no legitimate interest of the employer in controlling the progress and circumstances of work.

2. Maintaining a record of processing activities

In what cases is it necessary to maintain a record of data transfers (the type of data transferred, the recipient, the purpose, the precise date, and the employee actually carrying out the transfer)? Should the data transfer record include all data transfers, for example the sending of monthly attendance sheets or other data required by accountants?

Article 30 of the GDPR requires data controllers, or processors, to maintain a record of processing activities under their responsibility. Under Article 31 (1) of the GDPR, the record shall contain all of the following information:

a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;
b) the purposes of the processing;
c) a description of the categories of data subjects and of the categories of personal data;
d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;
e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;
f) where possible, the envisaged time limits for erasure of the different categories of data;
g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

Article 30 (1) d) explicitly states that the record to be maintained by the data controller shall include, as elements of obligatory content, the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations.

Article 30 (1) e) specifically emphasizes that the data controller shall include in the record it maintains, where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49 (1), the documentation of suitable safeguards.

Accordingly, the GDPR does not explicitly require data controllers to maintain detailed records of all data transfers, yet, under the principle of accountability provided for Article 5 (2), the data controller shall be able to demonstrate the lawfulness of data processing, which obligation it can best meet by recording all the details of personal data transfers.

Under Article 30 (5) of the GDPR, the obligation to maintain records (as a main rule) shall not apply to an enterprise or an organisation employing fewer than 250 persons **unless** the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, **the processing is not occasional**, or the processing includes special categories of data as referred to in Article 9(1) (e.g. health data) or personal data relating to criminal convictions and offences referred to in Article 10.

3. Legal bases of data processing

What can be a legal basis of the data processing?

Article 6 of the GDPR provides for the possible legal bases of data processing, i.e. the cases where data processing may be lawful:

Processing shall be lawful only if and to the extent that at least one of the following applies:

a) the **data subject has given consent** to the processing of his or her personal data for one or more specific purposes;
b) processing is **necessary for the performance of a contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
c) processing is **necessary for compliance with a legal obligation** to which the controller is subject;
d) processing is **necessary in order to protect the vital interests** of the data subject or of another natural person;
e) processing is necessary for the performance of a task carried out **in the public interest** or in the exercise of official authority vested in the controller;
f) processing is **necessary for the purposes of the legitimate interests pursued by the controller or by a third party**, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

4. Description of the STAR materials

Building on the needs of trainers, the EU data protection law has been divided into ten plus one topics by the STAR consortium. The topics were compiled by comparing the prioritized lists of topics from data protection authorities and other training stakeholders that emerged from the interviews the STAR consortium conducted (taking high priorities from both, as well as topics that occurred on both lists) identifying "must-have" topics on a logical basis. A preliminary list was then discussed and revised by all partners in the STAR consortium. The result is a list of modular topics which can be drawn upon to build a larger course on the GDPR. The training topics, structure and materials are developed with an objective of meeting the learners' needs, not just assuming from a lawyer's or a DPA's perspective what they think people need to know. The ten plus one topics are the following:

- **Topic 1 - Introduction to the European Union Data Protection Regime** - A topic on the basics of GDPR can be used to start sessions that then move to other specialist areas, and give a holistic overview of the field and introduces key legislation, definitions, as well as an overview of the GDPR concepts and its compliance requirements in terms of actions to be undertaken. Such general elements are an important precursor to specialised training, and for holistic understanding. The topic assumes that recipients have no previous (in-depth) knowledge in this area.
- **Topic 2 - Purposes and legal grounds for processing personal data** - An exploration of the main principles and various legal bases for the processing of personal data. The topic assists trainees in understanding their options in this space, including what is and what is not permitted, and which are the most appropriate legal grounds for their data processing. It also allows them to understand the approach they should have to GDPR compliance as a whole, due to the fact that the entire system is significantly based on these rules.
- **Topic 3 - The rights of the data subject and their exercise** - This topic explores the rights of the data subject in relation to the processing of their personal data, how organisations have an obligation to respect these and good practices to implement those rights in data processing. This material helps trainees to understand and protect the rights of data subjects, build systems and structures to help data subjects exercise their rights, and minimise their exposure to enforcement actions of administrative and/or contractual/tortious nature. That data controllers understand these rights is a priority topic for EU DPAs.
- **Topic 4 - Responsibilities of data controllers and processors** - An elaboration on the obligations of data controllers and processors in terms of transparency with data subjects and authorities, organisational measures to ensure compliance with the legislation, and actions to be undertaken in case of pathological situations, such as data breaches. It also explores the new principle of accountability, a cornerstone of the GDPR regime. This material is also critical for organisations to plan, achieve, and maintain GDPR compliance.
- **Topic 5 - Role of the DPO** - This topic explores one of the most relevant changes in the new regime, which is the obligation for some organisations to appoint a Data Protection Officer (DPO), a corporate role tasked with facilitating compliance with the GDPR provisions. It gives an overview on when and how to appoint one, and what DPOs are tasked with.
- **Topic 6 - Role of the DPA** - This topic explores the role and responsibilities of the key regulator under the GDPR, the Data Protection Authority (DPA). The topic entails questions like how can the DPA be of assistance to other data protection professionals? Trainees will be able to understand the role of the

DPA and how it likely interacts with their organization, how best to approach and work with the DPA and what can be expected of it.

- **Topic 7 - Technical and organisational measures** - This topic discusses one of the main subtopics of the responsibilities of data controllers and processors to give depth to one of the main instruments to ensure compliance with the new system, equipping trainees with the adequate knowledge to direct the implementation of these measures by technical experts in their organisation. It touches upon security of processing, information security, data minimization, anonymisation, pseudonymisation, Privacy-Enhancing-Technologies, data protection by design and by default, encryption, protection from intrusion, protection from loss, audit, penetration testing, and how such measures impact liability.
- **Topic 8 - Risk-based approach to data protection** - This topic explores the change of approach and culture in public and private organisations, the changing corporate cultures around processing of personal data and, respectively, how data protection impact assessments fit in. The topic focuses on ethics and correct approaches beyond simple compliance, with special attention to accountability and transparency.
- **Topic 9 - Data Protection Impact Assessments** - The GDPR introduces a new requirement around particular types of processing of personal data – the Data Protection Impact Assessment (DPIA). Essentially, for certain types of personal data processing that can be considered to pose a high risk to the rights and freedoms of data subjects, a data protection impact assessment exercise must be conducted prior to starting that processing. This topic introduces data protection impact assessment to the trainee (with special attention to DPIA concept; DPIA triggers; defining and identifying "high risk" processing; when and how to conduct a DPIA; validating DPIA results, the role of management and DPO, publishing a DPIA, usefulness for DPAs) and provide them with a methodological approach for conducting a DPIA.
- **Topic 10 - Data Protection Communication** - Much of the regulatory regime around data protection involves requirements for various forms of communication, for example, notifying affected parties and authorities in the case of data breach, or providing adequate information to data subjects so they can give informed consent to data process. This communication can be done well or done poorly, and this topic guides trainees in understanding their communications obligations and how to execute them.
- **Topic 11 - It's not just the GDPR** - This topic covers selected GDPR-related laws and special provisions - The GDPR does not stand alone but is rather accompanied and impacted by other EU legislation, national data protection legislation and decisions, and sectoral legislation. This training material works on embedding GDPR into the context of business and organisations by helping the trainees better understand these connections.

To facilitate the delivery of these topics, trainers are supported through additional materials and guidance. Trainers are supported by operational forms which can be used to host and deliver a training session. These supporting documents are created in generic, modular format to be edited as required by the trainer. The documents include:

- Attendance sheet
- Evaluation questionnaire
- GDPR compliance checklist
- Introductory one-page guide to the GDPR

The templates can be found in the Annexes of this handbook as well as on the website of the STAR project: http://www.project-star.eu/.

Besides the operational forms, a presentation has been developed in Microsoft PowerPoint format for each of the above referred topics. The materials focus predominantly on the GDPR and the respective legal framework of a European Union level, but indicates where national provisions are suggested to be highlighted. The materials are available only in English, however, end-users are encouraged to translate the materials into their national language(s) as they need it.

These presentations are easily adaptable and customizable to different audiences as well as to the specific needs of the trainer. Trainers are further assisted in the preparation for the training activity. In particular, in the notes-section below each slide useful information can be found (i.e. the trainer's guidance on how to tailor down the materials to meet the needs of the audience and the format of the training):

- 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].

It must be underlined that the slides are not applicable immediately as they require customization and preparation. The trainers are responsible for adjusting the training material to the level of expertise of the training recipients Prior to the delivery of the training:

- the expertise and background of the audience should be identified;
- 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 (a good level of expertise is expected from the trainer which can be further facilitated through the inclusion of the suggested reading materials);
- the slides that the trainer considers unnecessary should be reduced/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 other, more suitable (e.g. the organisation's) layout. Regardless of the changes in the layout, the training material should acknowledge the STAR project and its funding. The following text is advised to be used: "This material was developed by the STAR project, www.project-star.eu. (Support Training Activities on the data protection Reform; 2017-2019) and was 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." Further guidance for the use and display of the European Union flag in relation to this acknowledgement can be found at: https://ec.europa.eu/easme/en/communication-toolkit.

A categorisation has been also provided based on the depth and importance of the respective content by using differently coloured circles on 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 training materials are expected to be delivered in face-to-face training sessions as these remain common and in-demand with all data protection stakeholder groups. It is identified as useful, effective and an efficient way of introducing trainees to the materials as well as the best format for fostering interaction and discussion. It also has other benefits for DPAs including building working relationships. The effective delivery of training in this field is strongly influenced by several logistical factors in addition to the inherent nature of the training and the pedagogic strategies. This includes, for example, the time that trainees can take to receive training, travel to and from training locations. The STAR training materials are developed to fit within the time and logistical limits of face-to-face sessions. Furthermore, these training materials may also be used for online training as well (webinar or e-learning).

THE MICROSOFT POWERPOINT PRESENTATIONS IN .PPTX FORMAT ARE AVAILABLE IN THE FOLLOWING LINK:

HTTP://WWW.PROJECT-STAR.EU/TRAINING-MATERIALS

5. Using the STAR materials

Building on the needs of the target audience STAR developed GDPR training materials for DPAs and Data Protection Officers (DPOs) that are 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 and how the training materials are 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 Reports for the findings of the interviews and D2.4 List of Training Materials and associated report.[3]

Users of the STAR training materials can:

1. find the scenario that most closely matches their use for the training material,
2. use the scenario to identify any particular pedagogic approaches, practical considerations and the best ways to use the materials provided by STAR (e.g. which modules to use, any elements that can be removed, etc).

This section presents 8 training scenarios for Data Protection Authorities:

- New staff training at a data protection authority
- Specialist training for data protection authority staff
- DPAs training for Civil servants and public sector employees
- DPAs training judges
- DPA training (new) DPOs
- DPA training (experienced or established) DPOs
- DPA training for private sector (different sectors e.g. healthcare, education)
- Training to be published by a DPA for data controllers and processors

And 3 training scenarios for Data Protection Officers:

- DPO self-directed study
- DPO internal training for staff involved in data protection
- DPO internal training for staff not involved in data protection, but who may encounter data protection issues

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.

[3] http://www.project-star.eu/

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 to prepare for the training, and allow them to focus upon their organisational priorities and specific needs of the target audience. 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 put more emphasis on (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	Add national materials in the relevant, customisable slides

national differences.	
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 #1 or equivalent.
Why use STAR?	To reduce the time and effort required for the trainer to prepare for the training, 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 put more emphasis on (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	Please see individual slide topics
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 to prepare for the training, 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	Two 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 put more emphasis on (include key topics, and additional topics)	Topic 1 – Introduction to the European Union Data Protection Regime (if required). Topic 4 – responsibilities of data controllers and processors Topic 6 – the role of the data protection authority 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	Please 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 prepare for the training 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 put more emphasis on (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 7 – data protection in practice: Technical and organisational measures Topic 8 – Risk-based approach in the GDPR
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	Please see individual slide topics
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 put more emphasis on (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 Topic 3 –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	Please see individual slide topics
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 put more emphasis on (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 put more emphasis on (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 put more emphasis on (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	

Scenario #9 – DPO Self-directed study	
Capsule description	The STAR training materials are used by an appointed data protection officer to reinforce and improve their own knowledge. They are likely downloaded directly from the STAR project website and used at the DPOs own pace.
Trainer	Data protection officer (self)
Expected knowledge of Trainer	Moderate to high in data protection, may require some updating to GDPR issues. Interested in new developments in the GDPR and accessing/identifying best practice.
Trainee	As trainer
Expected knowledge of Trainee	As trainer
Why use STAR?	To access freely available, good-quality training materials, developed with the support of EU DPAs and DPOs.
Timing	One-hour sessions, broken up over several weeks of real time, fitted around other workload commitments of the trainee

Delivery format	Online, downloaded Microsoft 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 put more emphasis on (include key topics, and additional topics)	All (self-selected as required by the user, or taken in order)
Slides to use or remove	No need to remove any slides
Supporting material to use	
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	

Scenario #10 – DPO internal training for staff involved in data protection	
Capsule description	A DPO uses the STAR training materials to deliver training to staff in their organisation with specialist data protection related roles (e.g. IT, HR, communications, or within a DP team).
Trainer	DPO
Expected knowledge of Trainer	Moderate to high data protection knowledge
Trainee	DP-adjacent staff
Expected knowledge of Trainee	Low to moderate
Why use STAR?	To access freely available, good-quality training materials, developed with the support of EU DPAs and DPOs. To benefit from the specialised focus of some of the later STAR materials. To reduce the time and effort required for the trainer and allow them to focus upon their organisational priorities.
Timing	Multiple ½ day sessions
Delivery format	Small group discussions, mentor-led study
Self-directed or trained?	Hybrid – initial training sessions, followed up by self-directed use of the STAR materials.
Budgeting or other constraints	None
Special considerations (including pedagogic issues)	
STAR Modules to put more emphasis on (include key topics, and	All

additional topics)	
Slides to use or remove	
Supporting material to use	
How to specify for sector or national differences.	
Further adaption needed from trainer / host	Little customisation is strictly required, but the training materials could be adapted to include organisational policies and procedures (e.g. internal process for responding to a subject access request, DPO contacts, etc).
Additional reading	Please see individual slide topics
Other comments	

Scenario #11 – DPO internal training for staff not involved in data protection, but who may encounter data protection issues	
Capsule description	A DPO uses the STAR training materials as the starting point to roll out an organisation-wide data protection awareness training programme to ensure that all staff, even those without a data protection job element are aware of the organisation's responsibilities, policies and procedures around data protection.
Trainer	Organisational DPO
Expected knowledge of Trainer	Moderate to high
Trainee	All staff within an organisation (company, charity, etc)
Expected knowledge of Trainee	Potentially non-existent data protection knowledge.
Why use STAR?	To reduce the time and effort required for the trainer, and allow them to focus upon their organisational priorities.

	To access freely available, good-quality training materials, developed with the support of EU DPAs and DPOs.
Timing	1 hour
Delivery format	Webinars
Self-directed or trained?	Trained
Budgeting or other constraints	
Special considerations (including pedagogic issues)	
STAR Modules to put more emphasis on (include key topics, and additional topics).	Topic 1: Introduction to the EU Data protection regime
Slides to use or remove	
Supporting material to use	Intro to GDPR
How to specify for sector or national differences.	Examples can be changed to examples drawn from the specific experience of the training organisation.
Further adaption needed from trainer / host	Potentially substantial adaption. Trainer should include: Organisational data protection processes and policies (e.g. subject access requests, data breaches reporting process) Key contact details for reporting – e.g. DPO Any organisational "philosophy" for data protection and GDPR compliance.

Additional reading	None
Other comments	

6. Adapting the STAR materials to a trainers' specific needs

In the training materials themselves, several slides are marked with a purple dot in the top right corner, indicating that the specific slide requires adaption. In particular, the respective national provisions; sector-specific provisions; privacy policies; codes of conduct; further opinions or guidelines; and DPOs' specific responsibilities should be indicated when providing a training. The STAR consortium is interested in seeing the changes you make to these slides for your own industry or country, and would be willing to host edited versions of this handbook (e.g. translated, or nationally specific versions on our website). Therefore, the handbook is provided also in .doc format to enable its editing and re-use within organisational environments and as a completely formatted PDF in STAR branding for immediate dissemination and use.

6.1 Organisation

When the target audience is an employee or representative of a private organisation, we suggest to adjust the slides mentioned below, taken into consideration the following:

- DPOs own responsibility
- Privacy policy
- Codes of conduct
- Other opinions/guidelines

Topic	Slides to adjust
1. Introduction to data protection	**38** -Indicate the scope of the national data protection act
2. Purposes and legal grounds	-
3. Data subject rights	-
4. Controllers and processors	-
5. Role of the DPO	**11** - Is it mandatory or voluntary for your organization to designate a DPO? Give reasons why. **35, 36, 37** - Add the concrete tasks of your DPO at the organization. **43** - Present how does your organisation involve your DPO in all data protection related issues. **50** - Show the contact details of your DPO
6. Data Protection Authorities	**19** - You can add the contact information of your DPA

7. Technical and Organisational measures	**33** - Define the national rules concerning the notification of your DPA in case of a personal data breach
8. Risk based approach	**32** - If the organization has a risk register, provide contact details for the register-holder and the process for contributing to it. **37** - add any appropriate guidance on risk based approach from national DPA.
9. Data Protection Impact Assessments	**26** - If your organisation receiving training has an internal screening checklist or threshold criteria, present it here. **39** - include your DPO contact information on the "who to consult" slide
10. Data Protection Communication	**29** - Can be edited to present an organisation's own internal procedures for handling subject access requests.
11. Not just the GDPR - related	

6.2 Industry

When the target audience is a representative of an industry actor, we suggest to adjust the slides mentioned below, taken into consideration the respective sector-specific laws.

Topic	Slides to adjust for specific industry
1. Introduction to data protection	**38** -Indicate the scope of the national data protection act
2. Purposes and legal grounds	-
3. Data subject rights	-
4. Controllers and processors	-
5. Role of the DPO	**35, 36, 37 -** Are any specific tasks of a DPO in your business sector? Are there any sector specific data protection issues? (for example education, health care sector, finance sector.) **50 -** How can a company ensure that the information of its DPO is easily available for the data subjects / employees / supervisory authorities? Show examples for best practices (webpage of companies). **55 -** Expertise and skills of a DPO: besides the expertise in both national and European data protection laws and practices and an in-depth understanding of the GDPR what knowledge of the business sector is needed; give examples for specific business sectors

	63, 64 - How to choose a DPO? - You can add sector specific examples for the best practice to choose a DPO for a multinational or an SME
6. Data Protection Authorities	**19** - You can add the contact information of your DPA
7. Technical and Organisational measures	**33** - Define the national rules concerning the notification of your DPA in case of a personal data breach
8. Risk based approach	**37** - add any appropriate guidance on risk based approach from national DPA.
9. Data Protection Impact Assessments	**45** - You can add the specific company name to this slide's example of what bad publicity may look like. Also consider if there is any emerging tendency or method for publishing DPIA in this industry?
10. Data Protection Communication	**41** - approaches to algorithmic transparency - are there any good examples from industry peers? **66** - are there any GDPR/data protection codes of conduct applicable to this industry? What do these contain? **70** - are there any existing examples of GDPR certification, mark or seal schemes in this industry?
11. Not just the GDPR - related	

6.3 Country

One of the aims of the GDPR was to increase data protection harmonisation across the EU. However there are still 28 Member State laws, different legal environments and systems, and different policies adopted by data protection authorities. In addition, trainees are likely to be most receptive to guidance and sources of information available to them in native languages or that are produced by the supervisory authorities that will be responsible for regulating them. To this end, the generic STAR training materials can benefit from specification to the country where training is being delivered. The following table provides guidance on which slides in which training topics may need such adjustment. In many cases, this will include finding appropriate versions of information provided by national supervisory authorities. A list of national supervisory authorities is available here: https://edpb.europa.eu/about-edpb/board/members_en

Topic	Slides to adjust for country-specific information
1. Introduction to data protection	**38** -Indicate the scope of the national data protection act
2. Purposes and legal grounds	-

3. Data subject rights	-
4. Controllers and processors	-
5. Role of the DPO	**12** - define the concept of public authority or body under your national law **16** - Case studies regarding core activity: Can you add case studies from your national legislation? **18** - Case studies regarding large scale (& core activity): Can you add case studies from your national legislation? **23, 24** - Case studies: Regular and systematic monitoring: Can you add case studies from your national legislation? **30** - Does your country add more mandatory instances for the designation of a DPO? **46, 47** - How does your national legislation ensure the autonomy of a DPO? **49** - How is a DPO bound by secrecy or confidentiality in accordance with your national legislation? **50** - How should the designation of a DPO communicated to your national data protection authority? **59** - What are the requirements for certification of a DPO under your national law?
6. Data Protection Authorities	**10** - You can present the structure of your national DPA (organization chart, data of public interest, operation, legal status, ect) **12** - You can specify the measures taken by your country for the independent operation of a supervisory authority **14** - Add details on the appointment procedure of the members of the DPA in your country **19** - You can add the contact information of your DPA **24** - You can add information on how to lodge a complaint with your DPA, on legal remedies and other legal proceedings
7. Technical and Organisational measures	**33** - Define the national rules concerning the notification of your DPA in case of a personal data breach
8. Risk based approach	**37** - add any appropriate guidance on risk based approach from national DPA.
9. Data Protection Impact Assessments	**10** - context setting - Can replace with country-specific examples of big data protection-related scandals, that will resonate with your audience. **12** - Use definition of DPIA as published by national supervisory authority **24-25** - DPIA threshold criteria - if available, use a DPIA threshold criteria or checklist produced by your national supervisory authority. **33** - example DPIA process - can be replaced with example DPIA process suggested by national supervisory authorities (if available). As these are

	advisory, then it can still be useful to include other countries criteria for illustration or comparison. **47 -** Do you need to send DPIA to the DPA? - National supervisory authorities may have different requirements about when DPIAs need to be sent to them, and their policies relating to timing/responses when consultation is required may differ. Consult the website or published guidance from the national supervisory authority. **49** - DPIA tools - National supervisory authorities may produce their own DPIA tools.
10. Data Protection Communication	**24** - DPO contact information - Different national supervisory authorities have provided diverging guidance on the contact details required of the data protection officer. For some, this can be a generic email address (e.g. dpo@organisation) that will reach the data protection officer. Other supervisory authorities have produced guidance suggesting that a specific individual needs to be named as DPO, and their direct contact details provided. Trainers and trainees are encouraged to check guidance on the role of a DPO or on appointing a DPO from their national supervisory authority. **30** - has a list of national guidance on the right of access from a selection of supervisory authorities. More authorities may have published guidance on this topic since the slides were prepared, so please check your national supervisory authority. **49** - national data breach reporting process and requirements as set out by the data protection authority. **50** - has a list of national guidance on data breach notification from a selection of supervisory authorities. More authorities may have published guidance on this topic since the slides were prepared, so please check your national supervisory authority. **55** - insert national process for prior consultation, as published by national supervisory authority **56** - Do you need to send DPIA to the DPA? - National supervisory authorities may have different requirements about when DPIAs need to be sent to them, and their policies relating to publication. **72** - has a list of national guidance on data protection communication from a small selection of supervisory authorities. More authorities may have published guidance on this topic since the slides were prepared, so please check your national supervisory authority.
11. Not just the GDPR - related	

7. Annexes

This annex contains the operational forms, to be used while providing training on the GDPR. These forms not only assists trainers in organizing and carrying out the training, but also provides attendees useful information about the Regulation. In particular, STAR provides:

- an attendence sheet
- an evaluation questionnaire
- an introductory guide to the GDPR
- a GDPR compliance checklist

The operational forms are available in the following link:

Please note that the style of the document might have changed because of the format of the handbook, however the content remained unchanged. For the original documents please visit the website at http://www.project-star.eu/training-materials

STAR GDPR training sign in sheet			
Training Course		**Meeting Date:**	
Facilitator:		**Place/Room:**	

Name	Organisation	E-Mail	Signature

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

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

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.

To protect those rights, the GDPR empowers independent supervisory bodies (sometimes also called **Data Protection Authorities** or Information Commissioners) to oversee compliance with the GDPRand 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.

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.

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
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**

GDPR COMPLIANCE CHECKLIST

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

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 (any body 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[i] or on the list of processing activities that require a data protection impact assessment produced by national supervisory authorities.[ii]
- ☐ Conduct a data protection impact assessment[iii], 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[iv]
- ☐ 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[v]
- ☐ 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

[i] 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 public 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

[ii] 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

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**

[iii] See the Article 29 Working party Opinion WP268 on data protection impact assessment: https://ec.europa.eu/newsroom/document.cfm?doc_id=47711

[iv] https://trilateralresearch.co.uk/these-six-organisations-are-considering-appointing-a-dpo-and-yours/

[v] 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