

Training of Lawyers on European Data Protection Law 2 (TRADATA 2)

**Rights of the data subject, including rights in criminal
investigations and proceedings**

Filippo Bianchini

Barcelona, 21 April 2023



The project is co-financed with the support of the European Union's Justice programme

Training of Lawyers on EU Law relating to Data Protection 2



#TRADATA2

Main topics

- Data subject rights (DSR) – Introduction
- Common principles
- DSR & accountability
- A quick overview of the rights
- Focus on the right of access
- DSR and law enforcement directive
- DSR in the context of the European Data Strategy and the Digital services package

Some useful resources

[Opinion on some key issues of the Law Enforcement Directive \(EU 2016/680\) - wp258](#)

[Guidelines on Transparency under Regulation 2016/679 \(wp260rev.01\)](#)

[Guidelines 3/2019 on processing of personal data through video devices - Version 2.0 adopted on 29 January 2020](#)

[Guidelines on the right to "data portability" \(wp242rev.01\)](#)

[Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR \(part 1\) - Version 2.0 adopted on 7 July 2020](#)

[Guidelines 01/2022 on data subject rights - Right of access](#)

HANDBOOK

Handbook on European data protection law

2018 edition



Common principles

Data Subject rights - definitions

We all know the
definition of
Personal data...



We all know
who the Data
subject is...

Training of Lawyers on
EU Law relating to Data
Protection 2



#TRADATA2

DSAR Submitted

via one of a number of methods, including electronically (via email or website), by letter or by telephone. This may be received through any part of the organisation and is channelled through to the DPO.



DSAR Received and Logged

In the DSAR Register, which includes details such as the date received, due date for response; applicants details, information requested; details of decisions made in relation to access and any exemptions applied in respect of information not to be disclosed; and when and how the information is to be supplied, e.g. paper/electronic copies, postal method, etc.

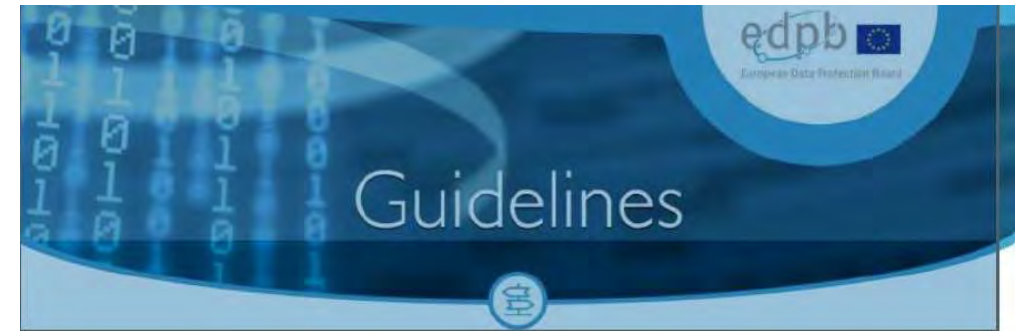


Verify the Identity of the Data Subject

Additional information may be requested to confirm identity. The Data Subject is informed that we will only keep a copy of the identity documents until the request has been fully processed and issued and all relevant review or appeal procedure timelines have expired. If the identity of the Data Subject cannot be confirmed the request is rejected and the reason for this communicated to the Data Subject.



- Need for identification
- if the controller has doubts about whether the data subject is who they claim to be, the controller must request additional information in order to confirm the identity of the data subject. The request for additional information must be proportionate to the type of data processed, the damage that could occur etc. in order to avoid excessive data collection.



Guidelines 01/2022 on data subject rights - Right of access

Version 1.0

Adopted on 18 January 2022



Evaluate Validity of Information Provided

If necessary, steps are taken to check the accuracy of the information provided by the Data Subject.



Identify and Compile the Personal Data

Data flow diagrams and data inventories are used to pinpoint the systems that store the requested personal data (if applicable). Staff are emailed to request any information that may be within their area regarding the request. The personal data is compiled.



Respond to Data Subject

The Data Subject is provided with a response and copies of any personal data capable of being provided.



Close DSAR

The fact that the request has been responded to is logged in the DSAR Register together with the date of closure.

Time limit to respond (art. 12)

As soon as possible - one month maximum

It can be extended by two further months where necessary, taking into account the complexity and number of the request

The data subject has to be informed about the reason for the delay

Formalities for the answer (art. 12)

Concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child.

In writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally

Importance of Legal Design

- Legal design is the application of human-centered design to the world of law, to make legal systems and services more human-centered, usable, and satisfying (M. Hagan)



In this introductory chapter, I introduce the concept of 'Legal Design' & define what Design and Design Thinking mean.

What is Legal Design?

Legal design is the application of human-centered design to the world of law, to make legal systems and services more human-centered, usable, and satisfying.



Can the request be refused (art. 12)?

- Yes, when it is manifestly unfounded or excessive;
- In such cases, a reasonable fee for such requests can be applied instead of the refusal
- These concepts have to be interpreted narrowly
- Burden of proof rests on the controller
- Restrictions may also exist in Member States' national law as (Art. 23 GDPR)



Video surveillance

- Given that any number of data subjects may be recorded in the same sequence of video surveillance a screening would then cause additional processing of personal data of other data subjects. If the data subject wishes to receive a copy of the material (article 15 (3)), this could adversely affect the rights and freedoms of other data subject in the material.
- If the video footage is not searchable for personal data, (i.e. the controller would likely have to go through a large amount of stored material in order to find the data subject in question) the controller may be unable to identify the data subject.
- Guidelines 3/2019



A quick overview of the rights

A quick summary of DSR (from the Handbook on European data protection law)

EU	Issues covered	CoE
Right to be informed		
General Data Protection Regulation, Article 12 CJEU, C-473/12, <i>Institut professionnel des agents immobiliers (IPI) v. Englebert</i> , 2013 CJEU, C-201/14, <i>Smaranda Bara and Others v. Casa Națională de Asigurări de Sănătate and Others</i> , 2015	Transparency of information	Modernised Convention 108, Article 8
General Data Protection Regulation, Article 13 (1) and (2) and Article 14 (1) and (2)	Content of information	Modernised Convention 108, Article 8 (1)
General Data Protection Regulation, Article 13 (1) and Article 14 (3)	Time of providing information	Modernised Convention 108, Article 9 (1) (b).
General Data Protection Regulation, Article 12 (1), (5) and (7)	Means of providing information	Modernised Convention 108, Article 9 (1) (b).
General Data Protection Regulation, Article 13 (2) (d) and Article 14 (2) (e), Articles 77, 78 and 79	Right to lodge a complaint	Modernised Convention 108, Article 9 (1) (f)

A quick
summary of DSR
(from the
Handbook on
European data
protection law)

Right of access

General Data Protection Regulation,
Article 15 (1)
CJEU, C-553/07, *College van
burgemeester en wethouders van*

Right of access to
one's own data

Modernised
Convention 108,
Article 9 (1) (b)
ECtHR, *Leander*

EU

Issues covered

CoE

CJEU, Joined cases C-141/12 and
C-372/12, *YS v. Minister voor
Immigratie, Integratie en Asiel and
Minister voor Immigratie, Integratie
en Asiel v. M and S*, 2014
CJEU, C-434/16, *Peter Nowak v. Data
Protection Commissioner*, 2017

Right to rectification

General Data Protection Regulation,
Article 16

Rectification
of inaccurate
personal data

Modernised
Convention 108,
Article 9 (1) (e)
ECtHR, *Cemalettin
Canli v. Turkey*,
No. 22427/04, 2008
ECtHR, *Ciubotaru v.
Moldova*, No. 27138/04,
2010

A quick summary of DSR (from the Handbook on European data protection law)

Right to rectification		
General Data Protection Regulation, Article 16	Rectification of inaccurate personal data	Modernised Convention 108, Article 9 (1) (e) ECtHR, <i>Cemalettin Canli v. Turkey</i> , No. 22427/04, 2008 ECtHR, <i>Ciubotaru v. Moldova</i> , No. 27138/04, 2010
Right to erasure		
General Data Protection Regulation, Article 17 (1)	The erasure of personal data	Modernised Convention 108, Article 9 (1) (e) ECtHR, <i>Segerstedt-Wiberg and Others v. Sweden</i> , No. 62332/00, 2006
CJEU, C-131/12, <i>Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González</i> [GC], 2014 CJEU, C-398/15, <i>Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni</i> , 2017	The right to be forgotten	

A quick
summary of DSR
(from the
Handbook on
European data
protection law)

Right to restriction of processing		
General Data Protection Regulation, Article 18 (1)	Right to restrict use of personal data	
General Data Protection Regulation, Article 19	Notification obligation	
Right to data portability		
General Data Protection Regulation, Article 20	Right to data portability	
Right to object		
General Data Protection Regulation, Article 21 (1) CJEU, C-398/15, <i>Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni</i> , 2017	Right to object due to the data subject's particular situation	Profiling Recommendation, Article 5.3 Modernised Convention 108, Article 9 (1) (d)

A quick summary of DSR (from the Handbook on European data protection law)

EU	Issues covered	CoE
General Data Protection Regulation, Article 21 (2)	Right to object to use of data for marketing purposes	Direct Marketing Recommendation, Article 4.1
General Data Protection Regulation, Article 21 (5)	Right to object by automated means	
Rights related to automated decision-making and profiling		
General Data Protection Regulation, Article 22	Rights related to automated decision-making and profiling	Modernised Convention 108, Article 9 (1) (a)
General Data Protection Regulation, Article 21	Rights to object automated decision-making	
General Data Protection Regulation, Article 13 (2) (f)	Rights to a meaningful explanation	Modernised Convention 108, Article 9 (1) (c)



Let's not forget data breaches

- Right to be informed in the event of a data breach, if the breach is likely to result in a high risk to the rights and freedoms of natural persons



DSR & accountability



DSR & accountability

- Question:
- What are the accountability measures to be taken for compliance with DSRs?




DSR and accountability

ICT systems able to respond quickly to DSRs (access, portability, erasure etc...) – art. 25

Microsoft Ignite

October 12-14, 2022

[Register now](#)

 **Microsoft** | [Learn](#) [Documentation](#) [Training](#) [Certifications](#) [Q&A](#) [Code Samples](#) [Shows](#) [Events](#)

[Sign in](#)

- Microsoft compliance offerings
- General Data Protection Regulation (GDPR)
 - GDPR overview
 - Recommended action plan for GDPR
 - Deploy information protection for data privacy regulations
 - Microsoft's data protection officer
- Accountability readiness checklists
- Data subject requests
 - Data subject requests
 - Manage data subject requests with the DSR case tool
 - Azure
 - Azure DevOps services
 - Dynamics 365
 - Intune
 - Microsoft Support & Professional Services
 - Office 365**

[Learn](#) / [General Data Protection Regulation \(GDPR\)](#) / [Data subject requests](#)

Office 365 Data Subject Requests for the GDPR and CCPA

Article • 09/27/2022 • 130 minutes to read • 5 contributors

Introduction to DSRs

The European Union [General Data Protection Regulation \(GDPR\)](#) gives rights to people (known in the regulation as *data subjects*) to manage the personal data that has been collected by an employer or other type of agency or organization (known as the *data controller* or just *controller*). Personal data is defined broadly under the GDPR as any data that relates to an identified or identifiable natural person. The GDPR gives data subjects specific rights to their personal data; these rights include obtaining copies of it, requesting changes to it, restricting the processing of it, deleting it, or receiving it in an electronic format so it can be moved to another controller. A formal request by a data subject to a controller to take an action on their personal data is called a *Data Subject Request* or DSR. The controller is obligated to promptly consider each DSR and provide a substantive response either by taking the requested action or by providing an explanation for why the DSR can't be accommodated by the controller. A controller should consult with its own legal or compliance advisors regarding the proper disposition of any given DSR.

In this article

- Introduction to DSRs
- Part 1: Responding to DSRs for Customer Data
- Using the Content Search eDiscovery tool to respond to DSRs
- Providing a copy of personal data

[Show more](#)

Adequate DSR policies (art. 24)

DSR and accountability

Data Subject Rights Policy

Operational Guide for Personnel

The Adoption Authority of Ireland



ÚDARÁS UCHTÁLA na hÉIREANN
THE ADOPTION AUTHORITY of IRELAND

Revision and Approval History					
Version	Revised By	Revision Date	Approved By	Approval Date	Comments
Draft	DPO	9/4/2019			
Reviewed	DPO	22/01/2020			
Reviewed	Matheson	19/10/2020			
Reviewed	DPO	28/01/2021			
Reviewed	DPO	1/04/2021			
Approved	Board	April 2021			



DSR and accountability

- Regulation of DSR requests in Data protection agreements (art. 28) & joint controller agreements (art. 26)
- Instructions and training for any person acting under the authority of the controller or of the processor who processes personal data
- ...

Focus on the right of access

The right of access

enshrined in Art. 8 of the EU Charter of Fundamental Rights.

Part of the European data protection legal framework since its beginning

Further developed by more specified and precise rules in Art. 15 GDPR.



Guidelines 01/2022 on data subject rights - Right of access

Version 1.0

Adopted on 18 January 2022

The right of access under the GDPR vs other access rights

Access to
public
documentation


FOIA requests



Does the request need a specific format?

- Controller must provide appropriate and user-friendly channels
- the data subject is not required to use these specific channels and may instead send the request to an official contact point of the controller
- No need for motivation

Employees' right of access: Italian SA fines Unicredit S.p.A. and orders corrective measures

 20 September 2022 [Italy](#)

Background information


- > Date of final decision: 16 June 2022
- > Controller: Unicredit S.p.A
- > Legal Reference: transparency and fairness of processing (Article 5.1(a)), transparency in and arrangements for exercise of DSR (Art.12), right of access (Art.15)
- > Decision: the Italian SA imposed an EUR 70,000 administrative fine and ordered the controller to grant the access request by the data subject
- > Key words: processing of data in the employment sector, right of access to one's personal data, transparency and fairness of processing




Summary of the Decision

Latest news

[Third fine imposed by Polish SA on the Surveyor General of Poland for failure to notify the personal data breach](#)

 23 September 2022 [Poland](#)

[Employees' right of access: Italian SA fines Unicredit S.p.A. and orders corrective measures](#)

 20 September 2022 [Italy](#)

[September plenary - adopted documents](#)

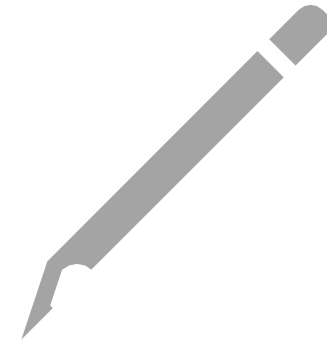
 20 September 2022 [EDPB](#)

[New EDPB opinion on certification criteria](#)

The right of access – overall aim



Provide individuals with sufficient, transparent and easily accessible information about the processing of their personal data so that they can be aware of and verify the lawfulness of the processing and the accuracy of the processed data.



Will facilitate the exercise of other rights such as the right to erasure or rectification.

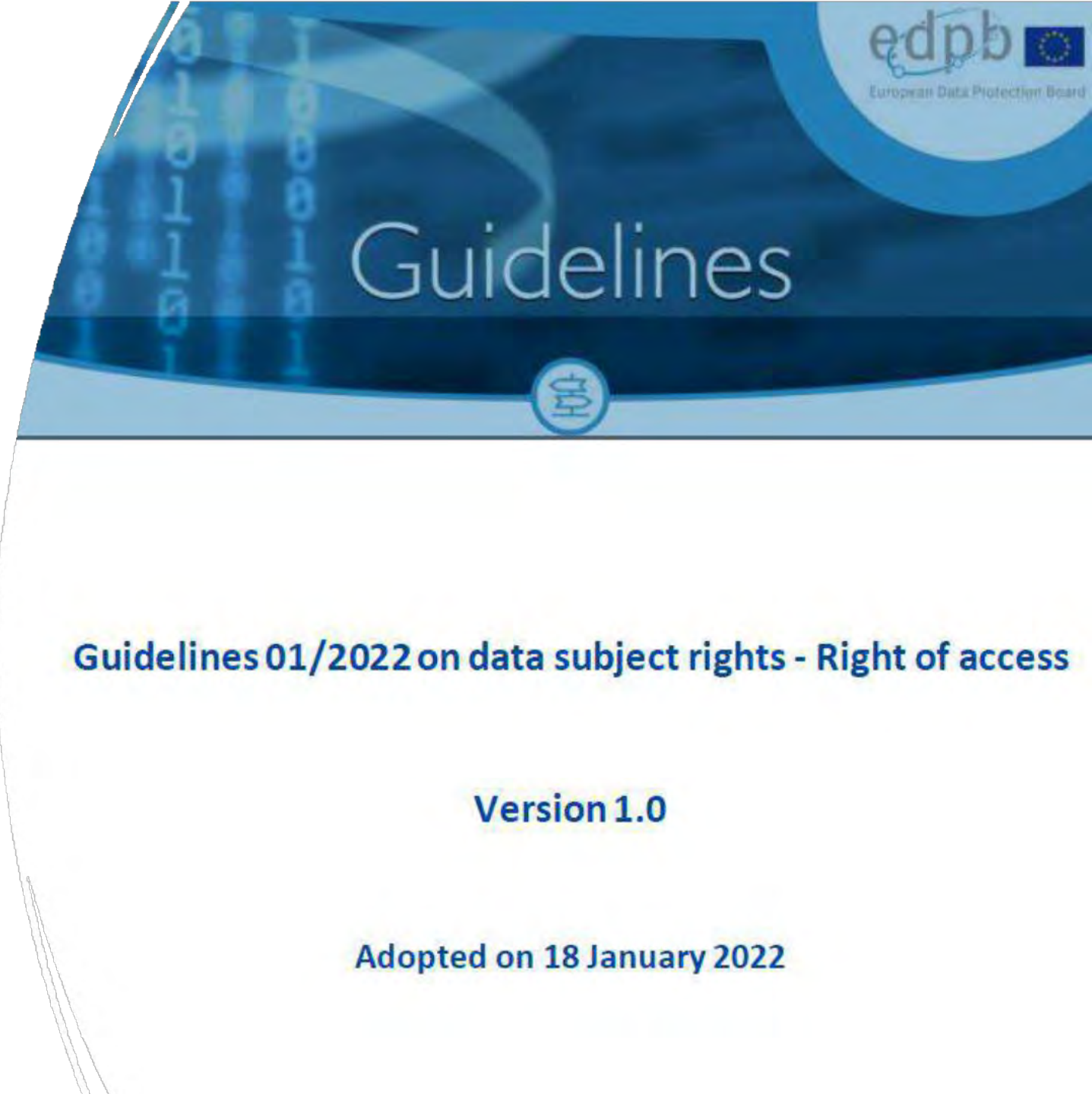
The right of access

three different components:

Confirmation as to whether data about the person is processed or not,

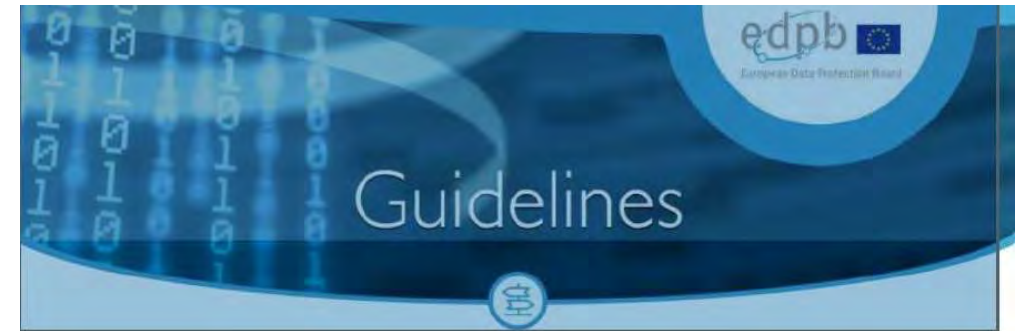
Access to this personal data and

Access to information about the processing, such as purpose, categories of data and recipients, duration of the processing, data subjects' rights and appropriate safeguards in case of third country transfers



Access to information about the processing vs transparency obligations of art. 13-14 GDPR

- Any information on the processing available to the controller may therefore have to be updated and tailored for the processing operations actually carried out with regard to the data subject making the request. Thus, referring to the wording of its privacy policy would not be a sufficient way for the controller to give information required by Art. 15(1)(a) to (h) and (2) unless the « tailored » information is the same as the « general » information.

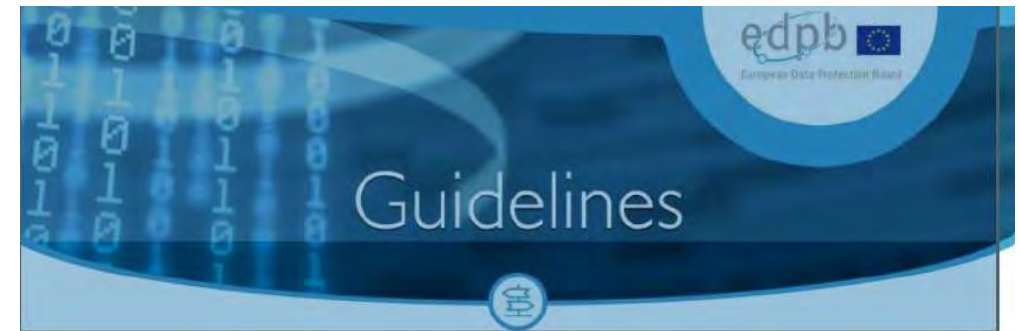


Guidelines 01/2022 on data subject rights - Right of access

Version 1.0

Adopted on 18 January 2022

- Unless explicitly stated otherwise, the request should be understood as referring to **all personal data concerning the data subject** and the controller may ask the data subject to specify the request if they process a large amount of data
- The communication of data and other information about the processing must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language
- Layered approach



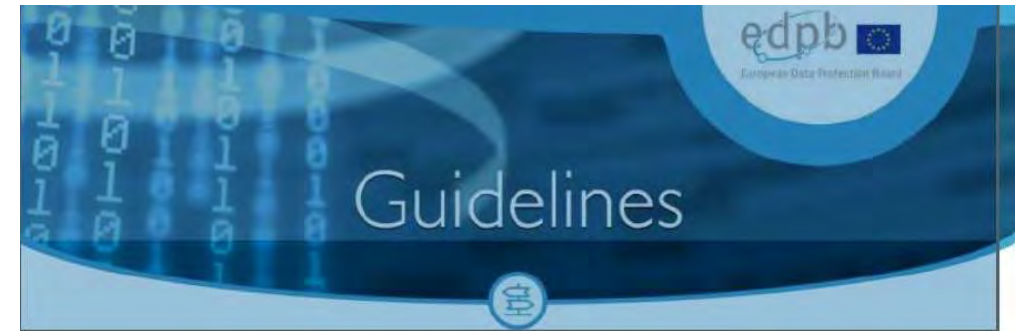
Guidelines 01/2022 on data subject rights - Right of access

Version 1.0

Adopted on 18 January 2022

Does it include inferred data?

- Data inferred from other data, rather than directly provided by the data subject (e.g. to assign a credit score or comply with anti-money laundering rules, algorithmic results, results of a health assessment or a personalization or recommendation process)
- the right of access includes both inferred and derived data, including personal data created by a service provider, whereas the right to data portability only includes data provided by the data subject.
- Therefore, in case of an access request and unlike a data portability request, the data subject should be provided not only with personal data provided to the controller in order to make a subsequent analysis or assessment about these data but also with the result of any such subsequent analysis or assessment.

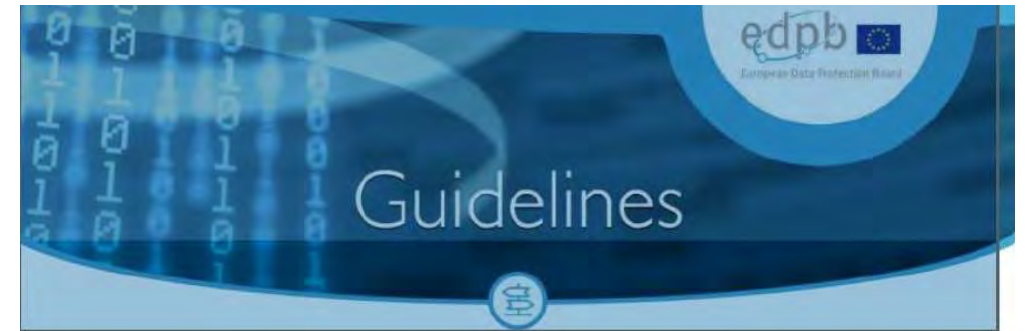


Guidelines 01/2022 on data subject rights - Right of access

Version 1.0

Adopted on 18 January 2022

- The right to obtain a copy shall not adversely affect the rights and freedoms of others (e.g. trade secrets, intellectual property, rights of other data subjects)
- Applying Art. 15(4) should not result in refusing the data subject's request altogether; it would only result in leaving out or rendering illegible those parts that may have negative effects for the rights and freedoms of others.



Guidelines 01/2022 on data subject rights - Right of access

Version 1.0

Adopted on 18 January 2022

- the controller is always obliged to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk of the processing
- Encryption is paramount, but access to data must be guaranteed



Guidelines 01/2022 on data subject rights - Right of access

Version 1.0

Adopted on 18 January 2022

Can DSR become a threat?

GDPR: When the Right to Access Personal Data Becomes a Threat

Luca Bufalieri, Massimo La Morgia, Alessandro Mei, Julinda Stefa
Department of Computer Science, Sapienza University of Rome, Italy

Email: bufalieri.l430586@studenti.uniroma1.it, {lamorgia, mei stef}@di.uniroma1.it

Abstract—After one year since the entry into force of the GDPR, all web sites and data controllers have updated their procedure to store users' data. The GDPR does not only cover how and what data should be saved by the service providers, but it also guarantees an easy way to know what data are collected and the freedom to export them.

In this paper, we carry out a comprehensive study on the right to access data provided by Article 15 of the GDPR. We examined more than 300 data controllers, performing for each of them a request to access personal data. We found that almost each data controller has a slightly different procedure to fulfill the request and several ways to provide data back to the user, from a structured file like CSV to a screenshot of the monitor. We measure the time needed to complete the access data request and the completeness of the information provided. After this phase of data gathering, we analyze the authentication process followed by the data controllers to establish the identity of the requester. We find that 50.4% of the data controllers that handled the request, even if they store the data in compliance with the GDPR, have flaws in the procedure of identifying the users or in the phase of sending the data, exposing the users to new threats. With the undesired and surprising result that the GDPR, in its present deployment, has actually decreased the privacy of the users of web services.

Index Terms—GDPR, Law Compliance, Privacy, Data Controllers, Web services

to a data controller. In our study, we target 334 of the most popular web sites according to the Alexa ranking. For the best of our knowledge, we are the first to conduct a comprehensive study on this topic with a world distribution of web sites, so our finding are also useful to refine previous works that took into account only one phase of the SAR [2], or used less rigorous methodologies to select the organizations [3], or could be biased by the small set of data controllers put under the lens [4].

We find that 19.6% of privacy policy pages are not compliant with the actual regulation. Then, we inquiry all the targeted web sites requiring our personal data. We study how the collectors identify the requester, we collect the response, and monitor the response time. In the end, we obtain our personal data from almost 65% of the targeted web sites, with a average time to fulfill the request of 16.4 days. Lastly, we checked the procedures used by the data controllers to fulfill the request. In this phase, we find several flaws that affect more than 32% of targeted data controller, and that could transform a fundamental right into a new and unpleasant threat.

This paper makes the following contributions:

- **World-wide snapshot:** We makes a world-wide snapshot of the actual deployment of the GDPR. We report on the

Blackhat USA 2019 Whitepaper

James Pavur and Casey Knerr

GDPArrrrr: Using Privacy Laws to Steal Identities

James Pavur*
DPhil Researcher
Oxford University

Casey Knerr
Security Consultant
Dionach LTD

DSR and law enforcement directive

DSR & Directive 2016/680

ARTICLE 29 DATA PROTECTION WORKING PARTY



17/EN

WP 258

Opinion on some key issues of the Law Enforcement Directive (EU 2016/680)

Adopted on 29 November 2017

Recommendations of the WP29

1. The Directive provides for a new architecture of the rights of data subjects, the principle being that they have a right to information, access, rectification, erasure or restriction of processing, unless these rights are restricted. Such restrictions shall only be possible where they constitute a necessary and proportionate measure and interpreted in a restrictive manner. Where these rights will have been restricted, Member States shall provide for the possibility for data subjects to exercise their rights through the competent supervisory authority which constitutes an additional safeguard for the data subjects.
2. The Directive states that Member States must provide for data subjects to have the right to obtain confirmation of processing and access to personal data being processed from the controller. The Directive does not allow for blanket restrictions to data subject rights.

DSR & EUROPOL REGULATION



EUROPEAN DATA PROTECTION SUPERVISOR

Decision of the European Data Protection Supervisor in complaint case 2020-0908 against the European Union Agency for Law Enforcement Cooperation (Europol)

Search the site [Donate](#)

EDRi [About us](#) [What we do](#) [Take action](#)

[Home](#) » [Resources](#) » [Rather delete than comply: how Europol snubbed data subject rights](#)

Rather delete than comply: how Europol snubbed data subject rights

On 8 September 2022, the European Data Protection Supervisor (EDPS) issued a decision ordering the EU law enforcement agency, Europol, to give Dutch activist Frank van der Linde access to the personal data the agency holds on him following a two-year investigation by the data protection watchdog. Findings of the inspection reveal that Europol tried to cover up the traces of the data processing and to avoid complying with the data access request by deleting van der Linde's data.

By EDRi | September 28, 2022

DSR in the context of the European Data Strategy and the Digital services package

Enhanced portability?

Digital Markets Act
(applies to the
Gatekeepers)

- provide effective portability of data generated through the activity of a business user or end user;

Data governance Act
(REGULATION (EU)
2022/868)

- Data intermediation services (providers of secure environment for individual and companies to share data)
- Personal data spaces (data wallets) for individuals to share their data

Data Act

- Measures to allow users of connected devices to gain access to data generated by them (freeing IoT data)
- Reinforced data portability right, both for personal and non-personal data

Training of Lawyers on European Data Protection Law 2 (TRADATA 2)

Data controller and data processor

Jordi Ferrer Guillén

Barcelona, 21 April 2023

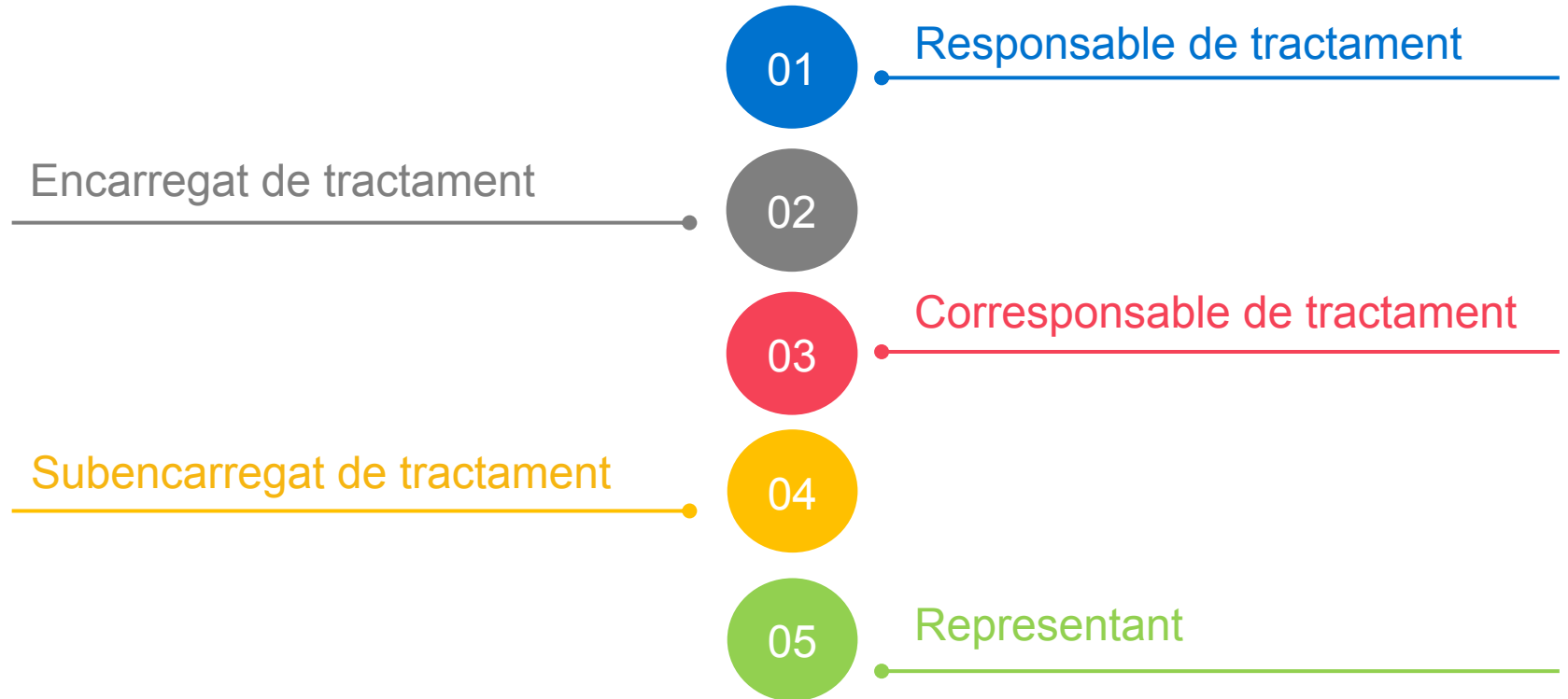


The project is co-financed with the support of the European Union's Justice programme

OBJECTIUS DE LA SESSIÓ

- 1** Identificar els intervinents obligats al compliment de la normativa de protecció de dades
- 2** Entendre el mapa d'intervinents en tractaments de dades
- 3** Avaluar riscos i les mesures exigibles a cada Responsable de Tractament.
- 3** Sistemes de demostració en compliment de protecció de dades
- 5** Processadors de Dades / Encarregats de Tractament: identificació i requeriments
- 6** Redactar i/o revisar el contracte d'Encarregat de Tractament

CONCEPTES



BIBLIOGRAFIA DE REFERENCIA

GRUPO DEL ARTÍCULO 29 SOBRE PROTECCIÓN DE DATOS



00264/10/ES
WP 169

Dictamen 1/2010 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento»

Adoptado el 16 de febrero de 2010



REGULACIÓ

El **CAPÍTOL IV del Reglament General de Protecció de Dades (RGPD)** regula la posició jurídica dels subjectes obligats Responsables del Tractament (RT) i Encarregat de Tractament (ET):

1. Responsabilitat del RT
2. Protecció de dades des del disseny i per defecte
3. Corresponsabilitat
4. Designació de responsables
5. ET i posició jurídica
6. Registre de les activitats de tractament

RESPONSABLES DEL TRACTAMENT (RT)



la persona física o jurídica, autoritat pública, servei o qualsevol altre organisme que,



sol o juntament amb d'altres,



determina



les finalitats i els mitjans



del tractament

RESPONSABLES DEL TRACTAMENT (RT)

Article 24 RGPD desenvolupa la Responsabilitat del RT:

1

GESTIÓ DEL RISC tenint en compte la naturalesa, l'àmbit, el context i les finalitats del tractament, així com els riscos de probabilitat i gravetat diversa per als drets i les llibertats de les persones físiques, el responsable del tractament ha d'aplicar les mesures tècniques i organitzatives adequades

Gestió del risc

Art. 32 RGPD

**SEGURETAT
DEL
TRACTAMENT**

(76) La probabilidad y la gravedad del riesgo para los derechos y libertades del interesado debe determinarse con referencia a la naturaleza, el alcance, el contexto y los fines del tratamiento de datos. El riesgo debe ponderarse sobre la base de una evaluación objetiva mediante la cual se determine si las operaciones de tratamiento de datos suponen un riesgo o si el riesgo es alto.

**Art. 30 RGPD
Registre
Activitats
Tractament**

**Art. 35 RGPD
EIPD**

RESPONSABLES DEL TRACTAMENT (RT)

Amb la gestió del risc avaluem impactes en relació a:

CONFIDENCIALITAT: impedeix la divulgació d' informació a individus, entitats o processos no autoritzats.

Assegurar l' accés a la informació únicament a aquelles persones que comptin amb la deguda autorització.

INTEGRITAT: mantenir les dades lliures de modificacions no autoritzades.

Comporta mantenir amb exactitud la informació tal qual va ser generada, sense ser manipulada ni alterada per persones o processos no autoritzats.

DISPONIBILITAT: garantir que la informació s' ha de trobar a disposició dels qui hi han d' accedir, ja siguin persones, processos o aplicacions.

L' accés a la informació i als sistemes per persones autoritzades ha de ser disponibles en el moment que així ho requereixin.

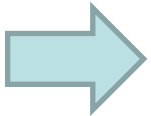
GESTIÓ DEL RISC

➤ Exemples de tractaments que comportin especials riscos recollits a l'article 28 LOPDGDD.

1. Quan el tractament pugui generar situacions de discriminació, usurpació d'identitat o frau, pèrdues financeres, dany per a la reputació, pèrdua de confidencialitat de dades subjectes al secret professional, reversió no autoritzada de la pseudonimització o qualsevol altre perjudici econòmic, moral o social significatiu per als afectats.
2. Quan el tractament pugui privar els afectats dels seus drets i llibertats o els pugui impedir l'exercici del control sobre les seves dades personals.
3. Quan es produeixi el tractament no merament incidental o accessori de les categories especials de dades a què es refereixen els articles 9 i 10 del Reglament (UE) 2016/679 i 9 i 10 d'aquesta Llei orgànica o de les dades relacionades amb la comissió d'infraccions administratives.
4. Quan el tractament impliqui una avaluació d'aspectes personals dels afectats amb la finalitat de crear o utilitzar perfils personals d'aquests, en particular mitjançant l'anàlisi o la predicció d'aspectes referits al seu rendiment a la feina, la seva situació econòmica, la seva salut, les seves preferències o interessos personals, la seva fiabilitat o comportament, la seva solvència financera, la seva localització o els seus moviments.

GESTIÓ DEL RISC

5. *Quan es dugui a terme el tractament de dades de grups d'afectats en una situació d'especial vulnerabilitat i, en particular, de menors d'edat i persones amb discapacitat.*
6. *Quan es produeixi un tractament massiu que impliqui un gran nombre d'afectats o comporti la recollida d'una gran quantitat de dades personals.*
7. *Quan les dades personals hagin de ser objecte d'una transferència, amb caràcter habitual, a tercers estats o organitzacions internacionals respecte dels quals no s'hagi declarat un nivell adequat de protecció*
8. *Qualsevol altres que segons el parer del responsable o de l'encarregat puguin tenir rellevància i en particular els previstos en codis de conducta i estàndards definits per esquemes de certificació.*



Innovació, tecnologia i gestió del risc

<https://www.aepd.es/es/areas-de-actuacion/innovacion-y-tecnologia>

https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_es?f%5B0%5D=opinions_topics%3A753

GESTIÓN DEL RIESGO

GRUPO "PROTECCIÓN DE DATOS" DEL ARTÍCULO 29



17/ES

WP 248 rev.01



Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679

Adoptadas el 4 de abril de 2017

Revisadas por última vez y adoptadas el 4 de octubre de 2017

Gestión del riesgo y evaluación de impacto en tratamientos de datos personales

Junio 2021



Esta obra está bajo una

SISTEMES DEMOSTRACIÓ COMPLIMENT

3

Possibles sistemes de demostració de compliment de les obligacions

Art. 40 RGPD

**ADHESIÓ CODIS
DE CONDUCTA**

Art. 42 RGPD

**MECANISME DE
CERTIFICACIÓ**

ADHESIÓ CODIS DE CONDUCTA

Art. 40 y 41 RGPD

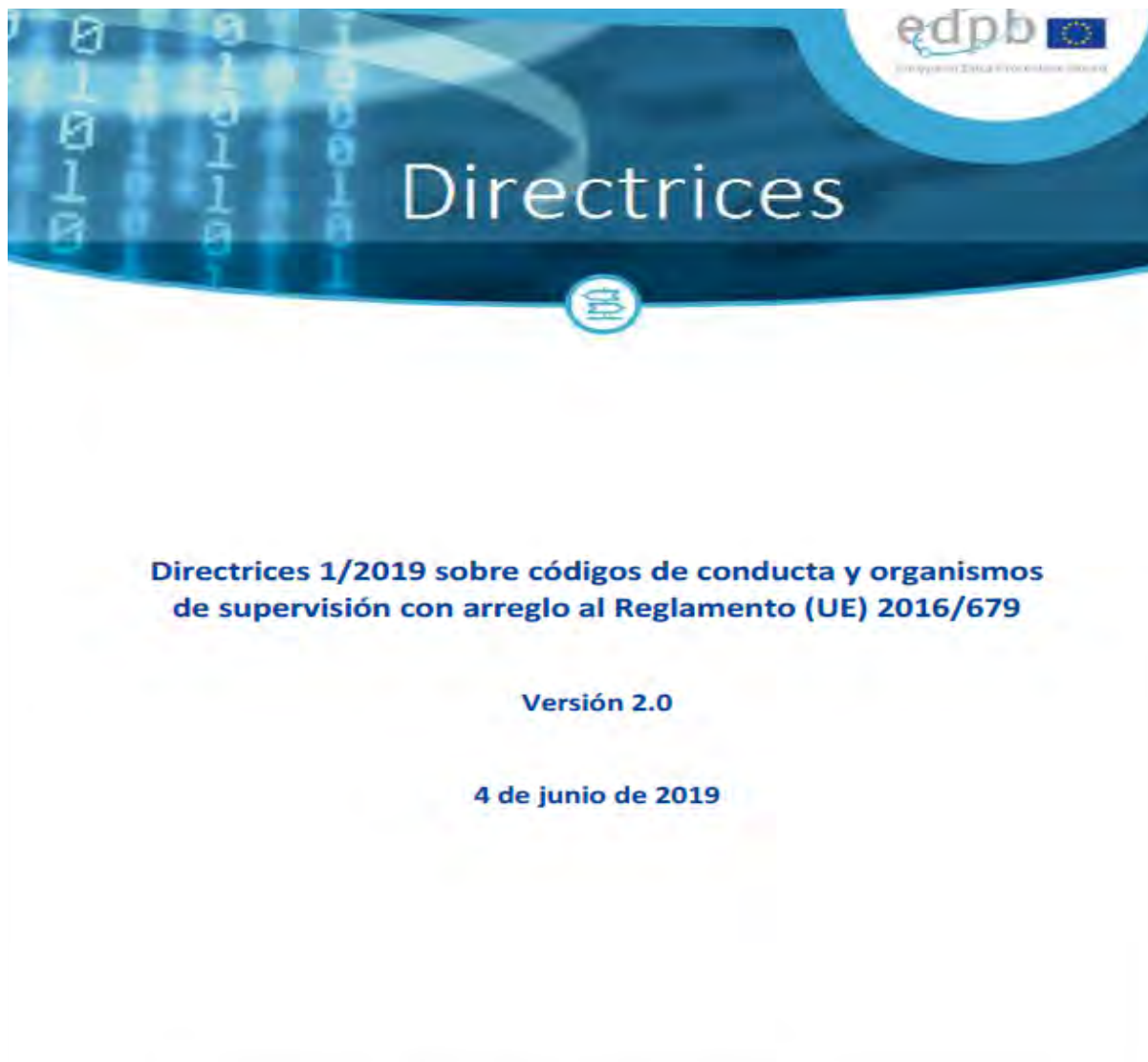
Sistema que es basa en l' autoregulació com a base de compliment RGPD

Impuls per a l' adhesió per part d' Associacions i Entitats representatives d' un determinat sector


Procés:

1. Presentació del projecte de Codi de conducta davant l' Autoritat de Control
2. Autoritat dictamina si és conforme al RGPD
3. Si és correcte i ajustat ho aprova
4. Registre dels codis de conducta aprovats i publicació per l' Autoritat de Control
5. Afectació a diversos estats: aplicació del mecanisme de coherència

ADHESIÓN CODIS DE CONDUCTA



ADHESIÓN CODIS DE CONDUCTA

 Última revisión: 17 de Enero de 2023

Registro de códigos de conducta

Año	Promotor	Denominación del Código	Resolución de aprobación y acreditación Organismo de Supervisión
2020	AUTOCONTROL	→ CÓDIGO DE CONDUCTA DE TRATAMIENTO DE DATOS EN ACTIVIDAD PUBLICITARIA → (english version)	→ 09/10/2020 28/11/2022 (Resolución Modificación)
2022	FARMAINDUSTRIA	→ CÓDIGO DE CONDUCTA REGULADOR DEL TRATAMIENTO DE DATOS PERSONALES EN EL ÁMBITO DE LOS ENSAYOS CLÍNICOS Y OTRAS INVESTIGACIONES CLÍNICAS Y DE LA FARMACOVIGILANCIA → (english version)	→ 10/02/2022
2022	UNESPA	→ CÓDIGO DE CONDUCTA REGULADOR DEL TRATAMIENTO DE DATOS PERSONALES EN LOS SISTEMAS COMUNES DEL SECTOR ASEGURADOR	→ 29/06/2022

MECANISMES DE CERTIFICACIÓ

Certificacions- Art. 42 y 43 RGPD

Sistema d' acreditació de compliment del Reglament

Característiques:

- Sistema voluntari i disponible per un procés transparent
- Expedició per organismes de certificació o per l' Autoritat de control
- S' atorga a responsable o encarregat per 3 anys i renovable
- Retirada de la certificació si no es compleixen els criteris de certificació

MECANISMES DE CERTIFICACIÓ

L' obtenció de la certificació per al responsable o encarregat NO LIMITA la seva responsabilitat.

Utilitats de la certificació:

- Acreditació del compliment del RGPD davant de tercers
- Mecanisme adequat per oferir garanties adequades per a transferències internacionals
- Control i sistema d' acreditació obligació in eligendo per a contractació d' encarregats de tractament

MECANISMES DE CERTIFICACIÓ



**Directrices 1/2018 sobre la certificación y la determinación
de los criterios de certificación de conformidad con los
artículos 42 y 43 del Reglamento**

Versión 3.0

4 de junio de 2019

CORRESPONSABILITAT DEL TRACTAMENT (CRT)

Art. 26 RGPD i art. 29 LOPDGDD desenvolupa la figura jurídica de corresponsabilitat:

Concepte: Dos o més RT determinen conjuntament objectius i mitjans del tractament.

Establiment d'acord o contracte entre els CRT on es reguli de forma transparent responsabilitats segons RGPD i en especial:

- Exercici de drets dels interessats
- Obligacions de subministrament informació
- Designació punt de contacte per als interessats

Transparència: punts essencials acord ha d' estar a disposició interessats

Llibertat exercici drets interessats davant qualsevol CRT: es dota de llibertat (finestra lliure de presentació)

REPRESENTANTS DE RT o ET no establerts en la UE (REP)

L' art. 27 RGPD i art. 30 LOPDGDD detalla alguns aspectes de la figura del Representant:

Obligació designa REP: a RT o ET d' aplicació territorial RGPD i NO establert a UE.

Excepcions designa REP:

Tractaments ocasionals sempre que no sigui de categories especials de dades

Organismes públics

Ubicació REP: establert en un Estat membre les dades del qual es tractin

Funcions REP: atendre consultes Autoritats i interessats sobre els tractaments.

Responsabilitat RT: designar REP no eximeix de responsabilitat el RT

Art. 30.2 LODPGDD: responsabilitat solidària danys i perjudicis en cas de responsabilitat a RT i REP

ENCARREGATS DEL TRACTAMENT (ET)

Regulació específica art. 28 RGPD I art. 33 LOPDGDD

Què?

- ✓ Què es un Encarregat del Tractament

Per què?

- ✓ Per què regular la figura de l'ET: prestació de serveis amb accés a dades

Com?

- ✓ Com ha de regular-se la relació entre RT y ET

ENCARREGATS DEL TRACTAMENT (ET)

Què?

L' ET és la persona física o jurídica, autoritat pública, servei o un altre organisme que presta un servei al responsable que comporta el tractament de dades personals per compte d' aquest.

Els tipus d' ET són tan variats com els tipus de serveis que puguin suposar accés a dades personals. Es poden intentar classificar en tipologies tals com:

Serveis informàtics

Serveis d' assessorament tipus gestoria

Serveis de consultoria diversa

Serveis de seguretat

Serveis d' analítica de dades

*Serveis sense accés a dades personals com serveis de neteja, manteniment

ENCARREGATS DEL TRACTAMENT (ET)

Què?

Es considera com a ET qualsevol prestador de serveis que comporti tractament de dades personals en el context de les activitats d' un establiment de l' ET a la Unió, independentment que el tractament tingui lloc a la Unió o no.

També s' aplicarà al tractament de dades personals d' interessats que resideixin a la Unió realitzat per un ET no establert a la Unió, quan les activitats de tractament estiguin relacionades amb:

- a) L' oferta de béns o serveis als dits interessats a la Unió, independentment de si se' ls requereix el seu pagament.
- b) El control del seu comportament, en la mesura que tingui lloc a la Unió.

ENCARREGATS DEL TRACTAMENT (ET)


Què?

Es muy probable que el RGPD aplique a cualquier uso que se haga de G Suite con fines empresariales, y por ello, queremos recordarte que debes realizar dos acciones importantes en tu cuenta de G Suite de [redacted] para facilitar tu cumplimiento con los requisitos de este reglamento. Te recomendamos que lleves a cabo las siguientes acciones cuanto antes:

1. Revisa y acepta las nuevas condiciones sobre el tratamiento de datos

Si el RGPD aplica al tratamiento de tus datos por parte de Google (p. ej., si tienes tu sede en un país miembro de la UE o si, aunque tu sede no esté en la UE, ofreces bienes o servicios a personas que residen en la UE), el contrato que suscribes con Google deberá incluir ciertas condiciones sobre el tratamiento de dichos datos. **A menos que aceptes la DPA 2.0, tu contrato no incluirá dichas condiciones.** Por lo tanto, te recomendamos que aceptes la DPA 2.0 en nombre de tu organización o consultes a un abogado. Te recordamos que el incumplimiento del RGPD está sujeto a importantes sanciones.


Para asegurarte de que tu contrato incluya las condiciones de la DPA 2.0 cuando el RGPD entre en vigor, por favor acepta la DPA 2.0 ahora a través de los siguientes pasos:

1. **Inicia sesión** en la [consola de administración](#) de Google.
2. Haz clic en .
3. Haz clic en **Cuenta** y haz clic en **Perfil de empresa**.
4. Selecciona **Perfil**.
5. Desplázate a la sección **Condiciones adicionales de seguridad y privacidad**, situada junto a la **Adenda sobre Tratamiento de Datos**, revisa la DPA 2.0 o pídele a la persona adecuada de tu organización que la revise, y haz clic en **Revisar y aceptar**.
6. Haz clic en **Aceptar**.

2. Introduce la información de contacto de tu delegado de protección de datos

Si tu organización está obligada por el RGPD a nombrar un delegado de protección de datos (DPD), Google deberá registrar su información de contacto para cumplir con los requisitos de dicho reglamento. En ese caso, deberás introducir esta información en la consola de administración. Si no estás seguro de si tu organización debe nombrar un DPD, te recomendamos que consultes a un abogado.

Para introducir la información de contacto del DPD, sigue estos pasos:

1. **Inicia sesión** en la [consola de administración](#) de Google.
2. Haz clic en .
3. Selecciona **Cuenta** y haz clic en **Perfil de empresa**.
4. Haz clic en **Mostrar Más** y selecciona **Información legal y de cumplimiento**.
5. En **Información sobre tu responsable de protección de datos**, introduce la información de contacto que se requiera.
6. Haz clic en **Guardar**.

En nuestro [sitio web sobre Google Cloud y el RGPD](#) encontrarás más información sobre este tema. Si tienes alguna pregunta, inicia sesión en la consola de administración para ponerte en contacto con el [equipo de protección de datos de Google Cloud](#).

ENCARREGATS DEL TRACTAMENT (ET)

Què?

L' ET executa tractaments, automatitzats o no, que el RT li hagi demanat formalment.

PUNT CLAU: determinar quan estem davant d' un ET o un altre tipus de relació jurídica:

1. El RT decideix sobre la finalitat i els usos de la informació
2. L' ET ha de complir amb les instruccions de qui li encomana un determinat servei, respecte al correcte tractament de les dades personals a les quals pugui tenir accés com a conseqüència de la prestació d' aquest servei.
3. L' ET adoptarà totes les decisions organitzatives i operacionals necessàries per a la prestació del servei
4. L' ET mai pot variar les finalitats i els usos de les dades ni les pot utilitzar per a les seves pròpies finalitats

ENCARREGATS DEL TRACTAMENT (ET)

Per qué?

L' ET tracta les dades personals **per compte del RT**.

El responsable té una obligació d' especial diligència en l' elecció i supervisió de l' encarregat

El RT no perd en cap cas la responsabilitat del correcte tractament de les dades personals i de la garantia dels drets de les persones afectades.

Deure de diligència i de supervisió en l' elecció i desenvolupament de l' ET.

S'ha de triar un encarregat del tractament que ofereixi garanties suficients respecte a la implantació i el manteniment de les mesures tècniques i organitzatives apropiades, segons el RGPD.

ENCARREGATS DEL TRACTAMENT (ET)

Per qué?

Exemple Check-list acreditació Deure de diligència i de supervisió en la elecció i desenvolupament de l'ET.

ID	PREGUNTA	RESPUESTA	ACREDITACIÓN
1	¿El Proveedor cumple adecuadamente con las obligaciones establecidas en la normativa de protección de datos?	SI	<i>Si es posible, aporte algún documento que confirme este extremo.</i>
2	¿El Proveedor dispone de una política o protocolo interno relativo a la gestión de derechos de los interesados?	SI	<i>Si la respuesta es afirmativa, deberá aportar copia de dichos procedimientos o protocolos.</i>
3	¿El Proveedor dispone de una política o protocolo interno para la gestión de brechas de seguridad?	SI	<i>Si la respuesta es afirmativa, deberá aportar copia de dichos procedimientos o protocolos.</i>
4	¿El Proveedor mantiene actualizado un Registro de Actividades de Tratamiento (RAT), incluyendo las realizadas por cuenta de terceros?	SI	
5	¿El Proveedor tiene la obligación legal de nombrar un Delegado de Protección de Datos? En caso de que la respuesta sea afirmativa, ¿Lo ha nombrado? por favor, incluya sus datos de contacto.	NO	<i>Si la respuesta es afirmativa, deberá acreditar el nombramiento con la copia de la notificación realizada en la sede electrónica de la AEPD. En determinados supuestos, no es obligatorio nombrar un DPO, por lo que el proveedor deberá acreditar por qué no es obligatorio nombrarlo en función de su actividad.</i>
6	¿El proveedor está adherido a algún código de conducta en materia de protección de datos (art. 40 RGPD)?	NO	<i>Si la respuesta es afirmativa, deberá aportar copia de dicha adhesión.</i>
7	¿El proveedor dispone de alguna certificación en materia de protección de datos a fin de demostrar el cumplimiento de lo dispuesto en el RGPD (art. 42 RGPD)?	NO	<i>Si la respuesta es afirmativa, deberá aportar copia de dicha certificación.</i>
8	¿El Proveedor cuenta con un departamento o área de seguridad o un Chief Security Officer?		<i>Si la respuesta es afirmativa, aporte sus datos de contacto.</i>
9	¿El Proveedor ha sido sancionado o inspeccionado en alguna ocasión por la Agencia Española de Protección de Datos o la autoridad de control equivalente?	NO	<i>Si la respuesta es afirmativa, deberá indicar el motivo, la graduación de la sanción y sanción impuesta, así como las medidas adoptadas para eliminar la causa del incumplimiento.</i>
10	¿Los servicios prestados por su compañía implican que los datos personales que se van a tratar en el marco de este contrato sean transferidos a un tercer país fuera del Espacio	NO	<i>En caso afirmativo, indique a qué país y las garantías o mecanismos legales (cláusulas contractuales tipo, BCR, excepciones previstas en la norma) adoptados por su</i>

ENCARREGATS DEL TRACTAMENT (ET)

Per qué?

Exemple Check-list acreditació Deure de diligència i de supervisió en la elecció i desenvolupament de l'ET.

30	¿Se va a utilizar alguna herramienta o plataforma para la prestación del servicio?	sí	
31	SÓLO SI SE HA RESPONDIDO AFIRMATIVAMENTE, POR FAVOR, COMPLETE LA SIGUIENTE INFORMACIÓN SOBRE LA INFORMACIÓN.		
32	PREGUNTA	RESPUESTA	
33	Nombre de la herramienta, plataforma o aplicación		
34	¿La herramienta, plataforma o aplicación se trata de un desarrollo propio de la empresa o se ha desarrollado por un tercero?		
35	En el caso de ser un desarrollo por un tercero, ¿se requiere de licencia para utilizarlo?		
36	¿De qué forma/s se lleva a cabo el intercambio de información entre la empresa y *****, y dentro de la misma empresa?		
37	¿Cómo se garantiza la segregación de funciones dentro de las herramienta, plataforma o aplicación en la prestación de/llos servicios (roles, privilegios, etc) como por ejemplo asignación de administradores, usuario, etc?		
38	¿Cuál es la política de contraseñas dentro de la herramienta?, ¿De qué forma garantizan que la contraseña sea robusta?		
39			
40	A) CUESTIONES DE PROTECCIÓN DE DATOS		
41	RESPUESTA	EVIDENCIA / Explicación	
42	L. Delegado de Protección de Datos (DPO)*	RESPUESTA	EVIDENCIA
43	¿Se ha procedido a nombrar y/o notificar, por el Proveedor, un DPO?		
44	Si la respuesta es SÍ, indique nombre e email del DPO.		Aportar evidencia de notificación a la autoridad de control
45	Si la respuesta es NO, por favor indique el motivo: a. El Proveedor no está legalmente obligado a nombrar un DPO.		
46	b. Si fuera otro motivo, especificarlo. [En caso de no especificar, **** considera que incumple el P. el requisito del RGPD]		
47	c. Si fuera otro interlocutor debido a las respuestas "a" o "b" anteriores, especificar cargo e email de contacto:		
48	Requisitos Proveedor		

ENCARREGATS DEL TRACTAMENT (ET)

Per qué?

- (81) Para garantizar el cumplimiento de las disposiciones del presente Reglamento respecto del tratamiento que lleve a cabo el encargado por cuenta del responsable, este, al encomendar actividades de tratamiento a un encargado, debe recurrir únicamente a encargados que ofrezcan suficientes garantías, en particular en lo que respecta a conocimientos especializados, fiabilidad y recursos, de cara a la aplicación de medidas técnicas y organizativas que cumplan los requisitos del presente Reglamento, incluida la seguridad del tratamiento. La adhesión del encargado a un código de conducta aprobado o a un mecanismo de certificación aprobado puede servir de elemento para demostrar el cumplimiento de las obligaciones por parte del responsable. El tratamiento por un encargado debe regirse por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros que vincule al encargado con el responsable, que fije el objeto y la duración del tratamiento, la naturaleza y fines del tratamiento, el tipo de datos personales y las categorías de interesados, habida cuenta de las funciones y responsabilidades específicas del encargado en el contexto del tratamiento que ha de llevarse a cabo y del riesgo para los derechos y libertades del interesado. El responsable y el encargado pueden optar por basarse en un contrato individual o en cláusulas contractuales tipo que adopte directamente la Comisión o que primero adopte una autoridad de control de conformidad con el mecanismo de coherencia y posteriormente la Comisión. Una vez finalizado el tratamiento por cuenta del responsable, el encargado debe, a elección de aquel, devolver o suprimir los datos personales, salvo que el Derecho de la Unión o de los Estados miembros aplicable al encargado del tratamiento obligue a conservar los datos.

La comunicació de dades personals, en el marc d' un acord d' ET, a un país que no formi part de la Unió es regeix per la regulació establerta en el RGPD per a les transferències internacionals.

ENCARREGATS DEL TRACTAMENT (ET)

Com?

La regulació de la relació entre el RT i l' ET s' ha d' establir a través de

- *un contracte*
- *o d' un acte jurídic similar que els vinculi.*

Contracte o acte jurídic ha de constar per **escrit**, inclòs en format electrònic.

La relació es pot articular a través d' un **acte jurídic unilateral** del RT.

Sector públic: resolució administrativa que consti notificada a l'encarregat del tractament.

En tot cas, el seu contingut ha de complir amb els requisits art. 28 RGPD.

ENCARREGATS DEL TRACTAMENT (ET)

Com?

Clausulat TIPUS

El contingut de l' acte o acord es pot basar en clàusules tipus establertes per:

1. La Comissió Europea,
2. per l' autoritat de control,
3. quan formin part d' una certificació atorgada al responsable o a l' encarregat del tractament

Página 1 de 18

Translations proofread by EDPB Members.
This language version has not yet been proofread.

Cláusulas contractuales tipo

A los efectos del artículo 28, apartado 3, del Reglamento 2016/679 (RGPD)

entre

[NOMBRE]
CVR [N° CVR]
[DIRECCIÓN]
[CÓDIGO POSTAL Y CIUDAD]
[PAÍS]

(el responsable del tratamiento)

y

[NOMBRE]
CVR [N° CVR]
[DIRECCIÓN]
[CÓDIGO POSTAL Y CIUDAD]
[PAÍS]

(encargado del tratamiento)

cada uno una «parte» y conjuntamente «las partes»

HAN ACORDADO las siguientes cláusulas contractuales (las Cláusulas) con el fin de cumplir los requisitos del RGPD y garantizar la protección de los derechos del interesado.

Cláusulas contractuales tipo de diciembre de 2019

ENCARREGATS DEL TRACTAMENT (ET)

Com?

El contracte o acte jurídic ha de recollir, com a mínim:

1. Objecte
2. Durada de la prestació
3. Naturalesa i la finalitat del tractament
4. Tipus de dades personals i categories d'interessats
5. Les obligacions i drets del RT
6. I en particular, per a l'ET en relació : .../...

ENCARREGATS DEL TRACTAMENT (ET)

Com?

1) Instruccions del RT

Documentar de forma precisa les instruccions respecte de l' encàrrec realitzat.

Identificar de forma clara els **tractaments de dades que cal realitzar** per l' ET, **atenent el tipus de servei prestat** i la forma de prestar-lo.

Determinar de forma clara les comunicacions a tercers que el responsable encomana a l' ET o que es deriven del servei prestat.

Salvaguarda per a ET que considera que alguna de les instruccions infringeix la normativa de PPDD, l' ET ha d' informar immediatament el RT.

ENCARREGATS DEL TRACTAMENT (ET)

Com?

2) Deure de confidencialitat de l' ET

Establir la forma en què l' ET garantirà que les persones autoritzades per tractar dades personals s' han compromès, de forma expressa, a respectar la confidencialitat, o subjecció a confidencialitat de naturalesa estatutària.

Per exemple: llistat de recursos i persones que tractaran les dades.

3) Mesures de seguretat aplicables per l' ET

L' acord haurà d' establir obligació de l' ET d' adoptar totes les mesures de seguretat necessàries, segons article 32 RGPD.

RT haurà dut a terme avaluació de riscos per avaluar les mesures de seguretat apropiades (es pot concretar les mesures o remissió estàndard)

L' ET també ha d' avaluar els possibles riscos derivats del tractament, atenent els recursos, mitjans, tecnologies que l' ET dugui a terme

3) Mesures de seguretat aplicables per l' ET

Implementar mesures tècniques i organitzatives apropiades per garantir el nivell de seguretat adequat al risc existent, i en tot cas:

1. la seudonimització
2. xifrat de dades personals
3. capacitat de garantir la confidencialitat, integritat, disponibilitat resiliència permanents dels sistemes i serveis de tractament
4. capacitat de restaurar la disponibilitat i l' accés a les dades personals en cas d' incident físic o tècnic
5. procés de verificació, avaluació i valoració regulars de l' eficàcia de les mesures tècniques i organitzatives per garantir la seguretat del tractament

ENCARREGATS DEL TRACTAMENT (ET)

Com?

4) Subcontractació ET (recórrer a un altre ET)

L' acord o contracte establirà el règim de subcontractació.

RGPD exigeix **autorització prèvia per escrit** del RT perquè l'ET pugui recórrer a SubET amb un sistema que pot ser

- específica amb identificació de l' entitat concreta
- general sense concretar i informant de la subcontractació perquè RT pugui, si s' escau, oposar-se

Règim del SubET amb les mateixes obligacions que ET.

Incompliment SubET: ET és responsable davant el RT de l' incompliment de les obligacions.

5) Exercici de drets dels interessats

Acord haurà d' establir si correspon a l' ET:

- atendre i donar resposta a les sol·licituds d'aquests drets per la qual cosa s'ha d'establir procediment per atendre'ls
- establir que es limitarà a comunicar al RT que s' ha exercit un dret i establir forma i termini que es comunicarà a l' ET

ENCARREGATS DEL TRACTAMENT (ET)

Com?

6) Suport en obligacions pròpies del RT

Es pot establir que l'ET sigui l'obligat (en nom del RT) a garantir compliment de les obligacions relatives a:

- notificació de violacions de dades a les Autoritats de Protecció de Dades
- comunicació de violacions de dades als interessats
- realització de les avaluacions d'impacte relativa la protecció de dades i de realització de consultes prèvies.

7) Destinació de les dades després de la prestació del servei

Contracte ha d' establir de forma clara quina de les dues opcions és l' escollida per l' RT, forma i el termini en què s' ha de complir respecte de les dades:

- ET ha de procedir a la supressió
- ET ha de procedir a la devolució de les dades
- ET pot conservar una còpia amb les dades degudament bloquejades, mentre puguin derivar-se responsabilitats de l' execució del servei.

8) Demostració de compliment per ET

Obligació de l' encarregat de posar a disposició del RT tota la informació necessària per demostrar el compliment de les obligacions establertes en el present article, així com per permetre i contribuir a:

- realització d' auditories
- inspeccions realitzades pel RT
- o per un altre auditor autoritzat pel RT.

Alguna pregunta més?

jordi.ferrer@icab.cat
jordi.ferrer@cyberlawconsulting.es

@JordiFerrerTwit

Training of Lawyers on European Data Protection Law 2 (TRADATA 2)

The principle of consent

Júlia Bacaria Gea

Barcelona, 21 April 2023



The project is co-financed with the support of the European Union's Justice programme



➤ **Things we have heard about CONSENT**

- It's always mandatory.
- If we don't consent they cannot use our personal data.
- You always have to accept the privacy policy (website frame).
- They cannot send us commercial electronic communications if we haven't previously consent.



➤ What we will learn today

- Consent is not always mandatory.
- The application of consent is residual.
- Is not a legal basis that should be prioritized over others.
- They may send us advertising or commercial electronic communications without consent.
- Privacy Policies do not have to be accepted.



➤ What we truly know about CONSENT (according to GDPR)

1. It's regulated in article 6.a) GDPR as a legal basis for processing.
2. It's regulated in article 7 GDPR:
 - The controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.
 - The data subject shall have the right to withdraw his or her consent at any time.
 - If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters.
3. And in Recital 32 GDPR:
 - Consent should be given by a clear affirmative act establishing a freely given, specific, informed.
 - When the processing has multiple purposes, consent should be given for all of them.
4. According to article 9 GDPR, consent might allow the processing of special categories of personal data.



➤ **What all these means?**

1. It's regulated in article 6.a) GDPR as a legal basis for processing.

- The data subject has given consent to the processing of his or her personal data for one or more specific purposes.
 - One legal basis of 6. Not the only one.
 - Law does not say that it has to be prioritized above the others.
 - Processing shall be lawful only if and to the extent that at least one of the following applies



2. It's regulated in article 7 GDPR

- The controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.
 - *If we don't sign a document, how can we prove consent?*
- The data subject shall have the right to withdraw his or her consent at any time.
- If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters.



3. Recital 32 GDPR:

- Consent should be given by a clear affirmative act establishing a freely given, specific, informed...
- ... and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement.
- Silence, pre-ticked boxes or inactivity should not therefore constitute consent.



4. According to article 9 GDPR

- Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.
- Paragraph 1 shall not apply if one of the following applies:
 - the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;



WHAT ABOUT THE REST OF THE PROCESSINGS?



WE NEED A LEGAL BASIS



IS THIS ONE CONSENT?



CASE 1 / EMPLOYEES

- SOMETIMES WE COME ACROSS COMPANIES THAT ASK THEIR EMPLOYEES FOR THEIR CONSENT TO PROCESS THEIR DATA. (FOR PURPOSES RELATED WITH THEIR JOB).
- THEY JUSTIFY IT SAYIN THAT THEY MUST PROCESS DATA FOR PAYROLL, CONTRACT, ETC.
- IF WE PROCESS THIS DATA ON THE BASIS OF CONSENT WE ARE NOT COMPLYING WITH THE REQUIREMENTS OF CONSENT.
 - CONSENT MUST BE INFORMED, FREE AND VOLUNTARY.
 - IF WE HAVE A SUPERIOR POSITION (EMPLOYER/EMPLOYEE) THE CONSENT CANNOT BE VOLUNTARY NOR FREE.
- THIS LEADS US TO BELIEVE THAT IT IS NOT THE CORRECT LEGAL BASE.
- IN THIS CASE THE LEGAL BASIS SHOULD BE THE CONTRACTUAL RELATION.



CASE 2 / CONTACT FORM WEBSITE

- COLLECTED DATA ARE IDENTIFYING DATA NOT SPECIAL CATEGORIES OF DATA.
- IF WE FULFILL A FORM AND INCLUDE OUR DATA WE ARE ALREADY GIVING CONSENT.
- RECITAL 32: CONSENT SHOULD BE GIVEN BY A CLEAR AFFIRMATIVE ACT ESTABLISHING A FREELY GIVEN, SPECIFIC, INFORMED AND UNAMBIGUOUS INDICATION OF THE DATA SUBJECT'S AGREEMENT TO THE PROCESSING OF PERSONAL DATA RELATING TO HIM OR HER, SUCH AS BY A WRITTEN STATEMENT, INCLUDING BY ELECTRONIC MEANS, OR AN ORAL STATEMENT.
 - IT IS NOT INCORRECT TO NOT TICKING A BOX
 - BUT IT CAN BE INCORRECT IF WHAT WE ACCEPT INCLUDES MANY PURPOSES
- SILENCE, PRE-TICKED BOXES OR INACTIVITY SHOULD NOT THEREFORE CONSTITUTE CONSENT.
- IN THIS CASE, LEGAL BASIS WILL BE UNAMBIGUOUS CONSENT.



CASE 3 / COMMERCIAL ELECTRONIC COMUNICATIONS

- IS A CONTROVERSIAL TOPIC.
- WE MUST DISTINGUISH BETWEEN CLIENTS OR OTHER KIND OF USERS.
- WITH CLIENTS WE HAVE A CONTRACTUAL RELATION (THIS IS THE LEGAL BASIS TO PROCESS THEIR DATA FOR THE PURPOSES RELATED WITH THE PRODUCT OR SERVICE THEY HAVE CONTRACTED.
- RECITAL 50: THE PROCESSING OF PERSONAL DATA FOR PURPOSES OTHER THAN THOSE FOR WHICH THE PERSONAL DATA WERE INITIALLY COLLECTED SHOULD BE ALLOWED ONLY WHERE THE PROCESSING IS COMPATIBLE WITH THE PURPOSES FOR WHICH THE PERSONAL DATA WERE INITIALLY COLLECTED.
- WE CAN USE THE LEGAL BASIS OF LEGITIMATE INTEREST (TALKING ABOUT PRIVATE COMPANIES)
- CLIENTS SHOULD BE ABLE TO UNSUBSCRIBE.
- THERE ARE OTHER REGULATIONS WICH ALSO REGULATE THIS COMMUNICATIONS.



OTHERS

- SHARING DATA WITH PROCESSORS: WE DON'T NEED A LEGAL BASIS, SO WE'LL NEVER NEED CONSENT TO DISCLOSE PERSONAL DATA FROM THE CONTROLLER TO THE PROCESSOR. PROCESSOR PROCESSES DATA AS IT WAS THE CONTROLLER, SO THE LEGAL BASIS IS THE SAME THAT THE CONTROLLER HAS DETERMINED.
- WHEN THERE ARE SPECIAL CATEGORIES OF DATA INVOLVED: WE NEED CONSENT BUT NOT ALWAYS. IT IS IMPORTANT TO LOOK AT THE OTHER EXCEPTIONS OF ARTICLE 9 GDPR.
- WHEN WE DON'T HAVE ANY PREVIOUS RELATION WITH THE DATA SUBJECT: WE CANNOT CONTACT NOR PROCESS DATA FROM ANYONE IF WE DON'T HAVE A LEGAL BASIS. IN THIS CASE, CONSENT MIGHT BE USEFUL.



➤ Conclusions

- CONSENT is not easy to comply
- We have to consider other legal basis before choosing CONSENT
- There are two types of consent: UNAMBIGUOUS CONSENT AND EXPLICIT CONSENT.



THANK YOU

Training of Lawyers on European Data Protection Law 2 (TRADATA 2)

Introduction to the GDPR

Xavier Urios Aparisi

Barcelona, 21 April 2023



The project is co-financed with the support of the European Union's Justice programme



Training of Lawyers on
EU Law relating to Data
Protection 2



#TRADATA2

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Article 99

Entry into force and application

1. This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.
2. It shall apply from 25 May 2018.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels, 27 April 2016.



- The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her.
- Art. 18 CE
 1. The right to honor, to personal and family privacy and to one's own image is guaranteed.
 4. The law will limit the use of information technology to guarantee the honor and personal and family privacy of citizens and the full exercise of their rights.





(4) The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality.

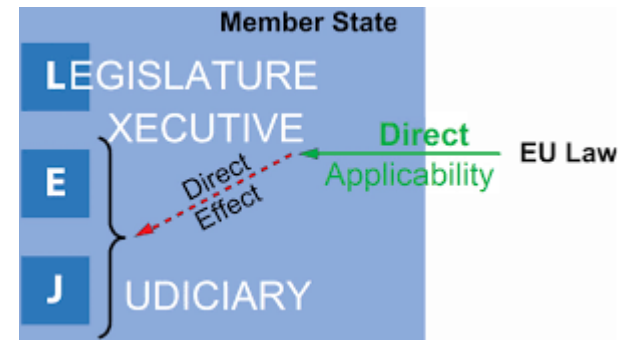
(13) In order to ensure a consistent level of protection for natural persons throughout the Union and to prevent divergences hampering the free movement of personal data within the internal market, a Regulation is necessary to provide legal certainty and transparency for economic operators, including micro, small and medium-sized enterprises, and to provide natural persons in all Member States with the same level of legally enforceable rights and obligations and responsibilities for controllers and processors, to ensure consistent monitoring of the processing of personal data, and equivalent sanctions in all Member States as well as effective cooperation between the supervisory authorities of different Member States



Training of Lawyers on EU Law relating to Data Protection 2



#TRADATA2





Training of Lawyers on EU Law relating to Data Protection 2



#TRADATA2





Training of Lawyers on EU Law relating to Data Protection 2



#TRADATA2

[CHAPTER I - General provisions](#)

[CHAPTER II - Principles](#)

[CHAPTER III - Rights of the data subject](#)

[CHAPTER IV - Controller and processor](#)

[CHAPTER V - Transfers of personal data to third countries or international organisations](#)

[CHAPTER VI - Independent supervisory authorities](#)

[CHAPTER VII - Cooperation and consistency](#)

[CHAPTER VIII - Remedies, liability and penalties](#)

[CHAPTER IX - Provisions relating to specific processing situations](#)

[CHAPTER X - Delegated acts and implementing acts](#)

[CHAPTER XI - Final provisions](#)



shutterstock.com • 1141192601



Article 1. Subject-matter and objectives

1. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.
2. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.
3. The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.



NO BORDERS



Training of Lawyers on EU Law relating to Data Protection 2



#TRADATA2





Training of Lawyers on
EU Law relating to Data
Protection 2



#TRADATA2

Art. 5.2 The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').





Article 24

Responsibility of the controller

1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.
2. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.
3. Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller.

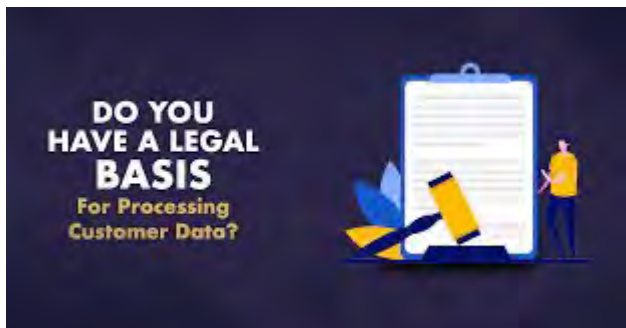
(art. 28 LOPD)



Article 32

Security of processing

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:
 - (a) the pseudonymisation and encryption of personal data;
 - (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
 - (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
 - (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.



Training of Lawyers on
EU Law relating to Data
Protection 2



#TRADATA2

- **Art. 6. Lawfulness of processing**

1. 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; (art. 8 LOPD)

(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.



Training of Lawyers on
EU Law relating to Data
Protection 2



#TRADATA2





Article 30 (art. 31 LOPD)

Records of processing activities

1. Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That 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).



2. 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, containing:
 - (a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;
 - (b) the categories of processing carried out on behalf of each controller;
 - (c) 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;
 - (d) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).
3. The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.
4. The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the supervisory authority on request.
5. The obligations referred to in paragraphs 1 and 2 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) or personal data relating to criminal convictions and offences referred to in Article 10.



Article 9

Processing of special categories of personal data

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





Article 25

Data protection by design and by default

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.
2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.
3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.



Article 35 (24)

Data protection impact assessment

1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.
2. The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.
3. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:
 - (a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
 - (b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or
 - (c) a systematic monitoring of a publicly accessible area on a large scale.
4. The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the Board referred to in Article 68.



Article 33

Notification of a personal data breach to the supervisory authority

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

Article 34

Communication of a personal data breach to the data subject

1. 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 undue delay.



Section 4

Data protection officer

Article 37

Designation of the data protection officer

1. The controller and the processor shall designate a data protection officer in any case where:

- (a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
- (b) 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; or
- (c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.

(art. 34 LOPD)



Training of Lawyers on EU Law relating to Data Protection 2



#TRADATA2

(91) This should in particular apply to large-scale processing operations which aim to process a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects and which are likely to result in a high risk, for example, on account of their sensitivity, where in accordance with the achieved state of technological knowledge a new technology is used on a large scale as well as to other processing operations which result in a high risk to the rights and freedoms of data subjects, in particular where those operations render it more difficult for data subjects to exercise their rights. A data protection impact assessment should also be made where personal data are processed for taking decisions regarding specific natural persons following any systematic and extensive evaluation of personal aspects relating to natural persons based on profiling those data or following the processing of special categories of personal data, biometric data, or data on criminal convictions and offences or related security measures. A data protection impact assessment is equally required for monitoring publicly accessible areas on a large scale, especially when using optic-electronic devices or for any other operations where the competent supervisory authority considers that the processing is likely to result in a high risk to the rights and freedoms of data subjects, in particular because they prevent data subjects from exercising a right or using a service or a contract, or because they are carried out systematically on a large scale. The processing of personal data should not be considered to be on a large scale if the processing concerns personal data from patients or clients by an individual physician, other health care professional or lawyer. In such cases, a data protection impact assessment should not be mandatory.



(24) The processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union should also be subject to this Regulation when it is related to the monitoring of the behaviour of such data subjects in so far as their behaviour takes place within the Union. In order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.



4. Infringements of the following provisions shall, in accordance with paragraph 2, 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:

- (a) the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43;
- (b) the obligations of the certification body pursuant to Articles 42 and 43;
- (c) the obligations of the monitoring body pursuant to Article 41(4). (art. 73 LOPD)

5. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

- (a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;
- (b) the data subjects' rights pursuant to Articles 12 to 22;
- (c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49;
- (d) any obligations pursuant to Member State law adopted under Chapter IX;
- (e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1). (art. 72 LOPD)



1. Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.
2. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:
 - (a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;
 - (b) the intentional or negligent character of the infringement;
 - (c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;
 - (d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;
 - (e) any relevant previous infringements by the controller or processor;
 - (f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;
 - (g) the categories of personal data affected by the infringement;
 - (h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;
 - (i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;
 - (j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and
 - (k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.



- xurios@gencat.cat



Training of Lawyers on
EU Law relating to Data
Protection 2



#TRADATA2

Training of Lawyers on European Data Protection Law 2 (TRADATA 2)

The principles in data protection

Caterina Bartrons

Barcelona, 21 April 2023



The project is co-financed with the support of the European Union's Justice programme



THE PRINCIPLES OF THE GDPR

- DATA PROTECTION BY DESIGN & DATA PROTECTION BY DEFAULT
- LAWFULNESS, FAIRNESS AND TRANSPARENCY
- PURPOSE LIMITATION
- DATA MINIMISATION
- ACCURACY
- STORAGE LIMITATION
- INTEGRITY AND CONFIDENCIALITY (SECURITY)
- ACCOUNTABILITY



TIMES ARE CHANGING

FROM DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

TO Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

- ✓ **Accountability**
- ✓ **Risk analysis: Identify and minimise the data protection risks**





EN English

Search

[Home](#) > [Law](#) > [Law by topic](#) > [Data protection](#) > [Reform of EU data protection rules](#) > [Rules for business and organisations](#) > [Principles of the GDPR](#)

Principles of the GDPR

For how long can data be kept and is it necessary to update it?

Rules on the length of time personal data can be stored and whether it needs to be updated under the EU's data protection rules.

How much data can be collected?

Rules on volumes of data that can be collected from individuals under the EU data protection law.

Overview of principles

Type of data that can be processed and conditions for processing.

Purpose of data processing

Can data be processed for any purpose?
Can we use data for another purpose?

What information must be given to individuals whose data is collected?

List of the type of information organisations must provide citizens with when collecting their data, this includes who is collecting it and why.





EN English

Search

Home > ... > Data protection > Reform of EU data protection rules > Rules for business and organisations > Enforcement and sanctions > Sanctions

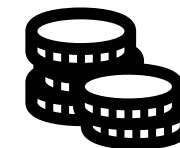
Sanctions

Can my company/my organisation be liable for damages?

Your organisation's liability for individual damages if you don't comply with the EU's data protection law.

What if my company/organisation fails to comply with the data protection rules?

A range of sanctions, including suspension of activities and fines can be imposed if your company doesn't comply with EU law on data protection.

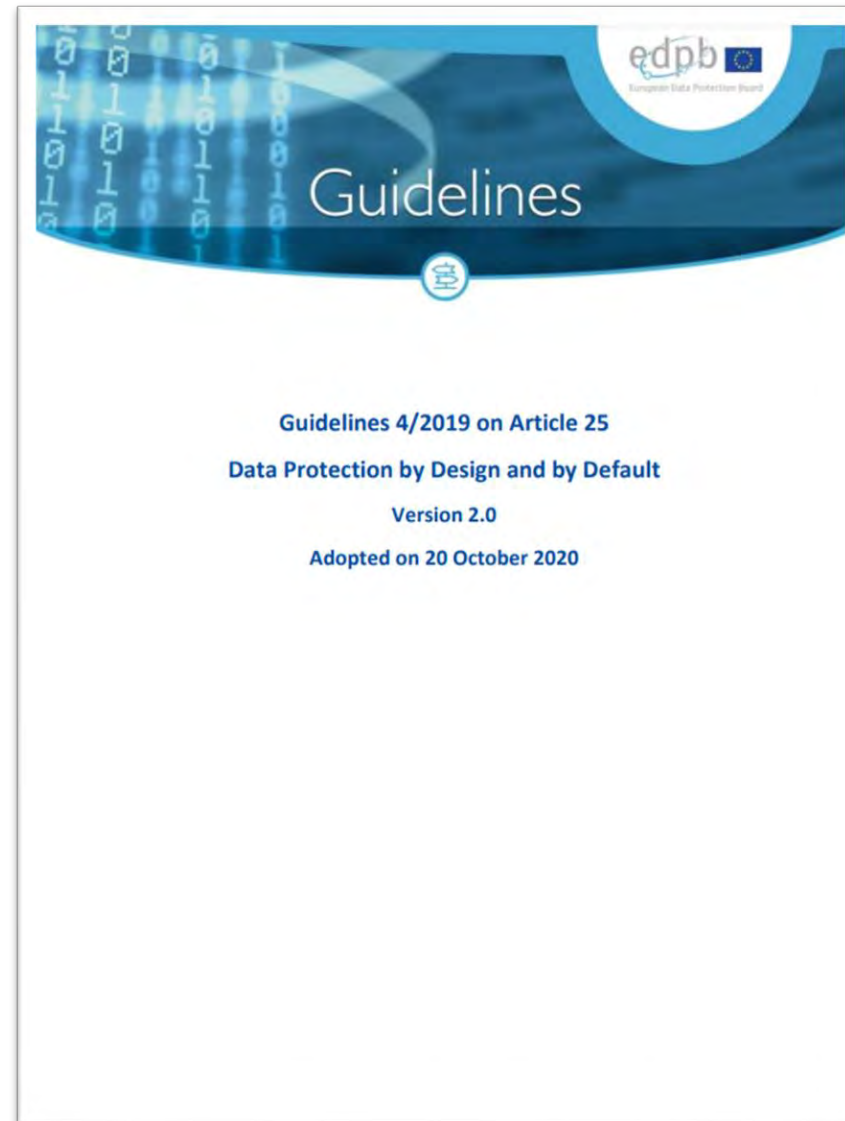


Training of Lawyers on EU Law relating to Data Protection 2



#TRADATA2

https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf





DATA PROTECTION BY DESIGN

Data protection by design is ultimately an approach that ensures you consider privacy and data protection issues at the design phase of any system, service, product or process and then throughout the lifecycle.

As expressed by the GDPR, it requires you to:

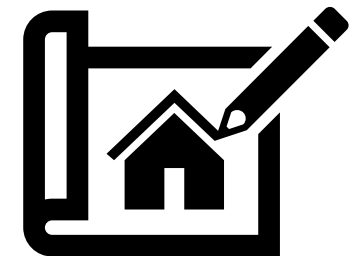
- ✓ put in place appropriate technical and organisational measures designed to implement the data protection principles effectively; and
- ✓ integrate safeguards into your processing so that you meet the GDPR's requirements and protect individual rights.

In essence this means you must integrate or 'bake in' data protection into your processing activities and business practices.

Data protection by design has broad application. Examples include:

- ✓ developing new IT systems, services, products and processes that involve processing personal data;
- ✓ developing organisational policies, processes, business practices and/or strategies that have privacy implications;
- ✓ physical design;
- ✓ embarking on data sharing initiatives; or
- ✓ using personal data for new purposes.

The underlying concepts of data protection by design are not new. Under the name 'privacy by design' they have existed for many years.





DATA PROTECTION BY DEFAULT

Data protection by default requires you to ensure that you only process the data that is necessary to achieve your specific purpose. It links to the fundamental data protection principles of data minimization and purpose limitation.

You have to process some personal data to achieve your purpose(s). Data protection by default means you need to specify this data before the processing starts, appropriately inform individuals and only process the data you need for your purpose. It does **not** require you to adopt a 'default to off' solution. What you need to do depends on the circumstances of your processing and the risks posed to individuals.

Nevertheless, you must consider things like:

- ✓ adopting a 'privacy-first' approach with any default settings of systems and applications;
- ✓ ensuring you do not provide an illusory choice to individuals relating to the data you will process;
- ✓ not processing additional data unless the individual decides you can;
- ✓ ensuring that personal data is not automatically made publicly available to others unless the individual decides to make it so; and
- ✓ providing individuals with sufficient controls and options to exercise their rights.





Who is responsible for complying with data protection by design and by default?

Article 25 specifies that, as the controller, you have responsibility for complying with data protection by design and by default. Depending on your circumstances, you may have different requirements for different areas within your organisation. For example:

- ✓ your senior management, eg developing a culture of 'privacy awareness' and ensuring you develop policies and procedures with data protection in mind;
- ✓ your software engineers, system architects and application developers, eg those who design systems, products and services should take account of data protection requirements and assist you in complying with your obligations; and
- ✓ your business practices, eg you should ensure that you embed data protection by design in all your internal processes and procedures.

This may not apply to all organisations, of course. However, data protection by design is about adopting an organisation-wide approach to data protection, and 'baking in' privacy considerations into any processing activity you undertake. It doesn't apply only if you are the type of organisation that has your own software developers and systems architects.

In considering whether to impose a penalty, the data protection authorities will take into account the technical and organisational measures you have put in place in respect of data protection by design.





What are we required to do?

You must put in place appropriate technical and organisational measures designed to implement the data protection principles effectively and safeguard individual rights.

There is no 'one size fits all' method to do this, and no one set of measures that you should put in place. It depends on your circumstances.

The key is that you consider data protection issues from the start of any processing activity and adopt appropriate policies and measures that meet the requirements of data protection by design and by default. Some examples of how you can do this include:

- ✓ minimising the processing of personal data;
- ✓ pseudonymising personal data as soon as possible;
- ✓ ensuring transparency in respect of the functions and processing of personal data;
- ✓ enabling individuals to monitor the processing; and
- ✓ creating (and improving) security features.

This is not an exhaustive list. Complying with data protection by design and by default may require you to do much more than the above.

However, we cannot provide a complete guide to all aspects of data protection by design and by default in all circumstances. This guidance identifies the main points for you to consider.

Depending on the processing you are doing, you may need to obtain specialist advice that goes beyond the scope of this guidance.





When should we do this?

Data protection by design starts at the initial phase of any system, service, product, or process. You should begin by considering your intended processing activities, the risks that these may pose to individuals, and the possible measures available to ensure that you comply with the data protection principles and protect individual rights. These considerations must cover:

- ✓ the state of the art and costs of implementation of any measures;
- ✓ the nature, scope, context and purposes of your processing; and
- ✓ the risks that your processing poses to the rights and freedoms of individuals.

This is similar to the information risk assessment you should do when considering your security measures.

These considerations lead into the second step, where you put in place actual technical and organisational measures to implement the data protection principles and integrate safeguards into your processing.

This is why there is no single solution or process that applies to every organisation or every processing activity, although there are a number of commonalities that may apply to your specific circumstances as described below.

The GDPR requires you to take these actions:

- ✓ ‘at the time of the determination of the means of the processing’ – in other words, when you are at the design phase of any processing activity; and
- ✓ ‘at the time of the processing itself’ – ie during the lifecycle of your processing activity.





How do we do this in practice?

How you go about doing this depends on your circumstances – who you are, what you are doing, the resources you have available, and the nature of the data you process. You may not need to have a set of documents and organisational controls in place, although in some situations you will be required to have certain documents available concerning your processing.

The key is to take an organisational approach that achieves certain outcomes, such as ensuring that:

- ✓ you consider data protection issues as part of the design and implementation of systems, services, products and business practices;
- ✓ you make data protection an essential component of the core functionality of your processing systems and services;
- ✓ you only process the personal data that you need in relation to your purposes(s), and that you only use the data for those purposes;
- ✓ personal data is automatically protected in any IT system, service, product, and/or business practice, so that individuals should not have to take any specific action to protect their privacy;
- ✓ the identity and contact information of those responsible for data protection are available both within your organisation and to individuals;
- ✓ you adopt a 'plain language' policy for any public documents so that individuals easily understand what you are doing with their personal data;
- ✓ you provide individuals with tools so they can determine how you are using their personal data, and whether you are properly enforcing your policies; and
- ✓ you offer strong privacy defaults, user-friendly options and controls, and respect user preferences.

Many of these relate to other obligations in the UK GDPR, such as transparency requirements, documentation, Data Protection Officers and DPIAs. This shows the broad nature of data protection by design and how it applies to all aspects of your processing. Our guidance on these topics will help you when you consider the measures you need to put in place for data protection by design and by default.





PRINCIPLES

The GDPR sets out seven key principles (art. 5):

- ✓ Lawfulness, fairness and transparency
- ✓ Purpose limitation
- ✓ Data minimization
- ✓ Accuracy
- ✓ Storage limitation
- ✓ Integrity and confidentiality (security)
- ✓ Accountability



These principles should lie at the heart of your approach to processing personal data.



Why are the principles important?

The principles lie at the heart of the GDPR.

They are set out right at the start of the legislation and inform everything that follows.

They don't give hard and fast rules, but rather embody the spirit of the general data protection regime - and as such there are very limited exceptions.

Compliance with the spirit of these key principles is therefore a fundamental building block for good data protection practice. It is also key to your compliance with the detailed provisions of the GDPR.

Failure to comply with the principles may leave you open to substantial fines.





LAWFULNESS, FAIRNESS AND TRANSPARENCY

- ✓ You must identify valid grounds under the GDPR (known as a 'lawful basis') for collecting and using personal data.
- ✓ You must ensure that you do not do anything with the data in breach of any other laws.
- ✓ You must use personal data in a way that is fair. This means you must not process the data in a way that is unduly detrimental, unexpected or misleading to the individuals concerned.
- ✓ You must be clear, open and honest with people from the start about how you will use their personal data.

Checklist:

Lawfulness

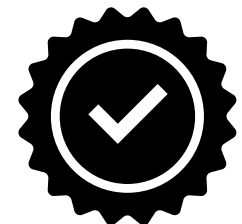
- ☐ We have identified an appropriate lawful basis (or bases) for our processing.
- ☐ If we are processing special category data or criminal offence data, we have identified a condition for processing this type of data.
- ☐ We don't do anything generally unlawful with personal data.

Fairness

- ☐ We have considered how the processing may affect the individuals concerned and can justify any adverse impact.
- ☐ We only handle people's data in ways they would reasonably expect, or we can explain why any unexpected processing is justified.
- ☐ We do not deceive or mislead people when we collect their personal data.

Transparency

- ☐ We are open and honest and comply with the transparency obligations of the right to be informed.





PURPOSE LIMITATION

- ✓ You must be clear about what your purposes for processing are from the start.
- ✓ You need to record your purposes as part of your documentation obligations and specify them in your privacy information for individuals.
- ✓ You can only use the personal data for a new purpose if either this is compatible with your original purpose, you get consent, or you have a clear obligation or function set out in law.

Checklist

- ☐ We have clearly identified our purpose or purposes for processing.
- ☐ We have documented those purposes.
- ☐ We include details of our purposes in our privacy information for individuals.
- ☐ We regularly review our processing and, where necessary, update our documentation and our privacy information for individuals.
- ☐ If we plan to use personal data for a new purpose other than a legal obligation or function set out in law, we check that this is compatible with our original purpose, or we get specific consent for the new purpose.





DATA MINIMISATION

You must ensure the personal data you are processing is:

- ✓ adequate – sufficient to properly fulfil your stated purpose;
- ✓ relevant – has a rational link to that purpose; and
- ✓ limited to what is necessary – you do not hold more than you need for that purpose.

Checklist

- ☐ We only collect personal data we actually need for our specified purposes.
- ☐ We have sufficient personal data to properly fulfil those purposes.
- ☐ We periodically review the data we hold and delete anything we don't need.



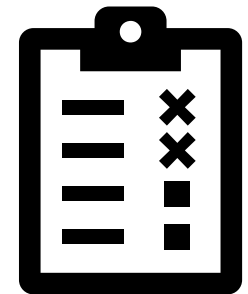


ACCURACY

- ✓ You should take all reasonable steps to ensure the personal data you hold is not incorrect or misleading as to any matter of fact.
- ✓ You may need to keep the personal data updated, although this will depend on what you are using it for.
- ✓ If you discover that personal data is incorrect or misleading, you must take reasonable steps to correct or erase it as soon as possible.
- ✓ You must carefully consider any challenges to the accuracy of personal data.

Checklist

- ☐ We ensure the accuracy of any personal data we create.
- ☐ We have appropriate processes in place to check the accuracy of the data we collect, and we record the source of that data.
- ☐ We have a process in place to identify when we need to keep the data updated to properly fulfil our purpose, and we update it as necessary.
- ☐ If we need to keep a record of a mistake, we clearly identify it as a mistake.
- ☐ Our records clearly identify any matters of opinion, and where appropriate whose opinion it is and any relevant changes to the underlying facts.
- ☐ We comply with the individual's right to rectification and carefully consider any challenges to the accuracy of the personal data.
- ☐ As a matter of good practice, we keep a note of any challenges to the accuracy of the personal data.





STORAGE LIMITATION

- ✓ You must not keep personal data for longer than you need it.
- ✓ You need to think about – and be able to justify – how long you keep personal data. This will depend on your purposes for holding the data.
- ✓ You need a policy setting standard retention periods wherever possible, to comply with documentation requirements.
- ✓ You should also periodically review the data you hold, and erase or anonymise it when you no longer need it.
- ✓ You must carefully consider any challenges to your retention of data. Individuals have a right to erasure if you no longer need the data.
- ✓ You can keep personal data for longer if you are only keeping it for public interest archiving, scientific or historical research, or statistical purposes.

Checklist

- ☐ We know what personal data we hold and why we need it.
- ☐ We carefully consider and can justify how long we keep personal data.
- ☐ We have a policy with standard retention periods where possible, in line with documentation obligations.
- ☐ We regularly review our information and erase or anonymise personal data when we no longer need it.
- ☐ We have appropriate processes in place to comply with individuals' requests for erasure under 'the right to be forgotten'.
- ☐ We clearly identify any personal data that we need to keep for public interest archiving, scientific or historical research, or statistical purposes.



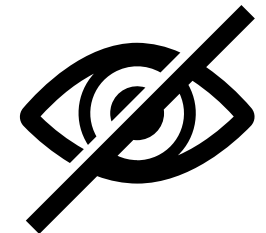


INTEGRITY AND CONFIDENTIALITY (SECURITY)

You must ensure that you have appropriate security measures in place to protect the personal data you hold.

This is the 'integrity and confidentiality' principle of the GDPR – also known as the security principle.

- ✓ A key principle of the GDPR is that you process personal data securely by means of 'appropriate technical and organisational measures' – this is the 'security principle'.
- ✓ Doing this requires you to consider things like risk analysis, organisational policies, and physical and technical measures.
- ✓ You also have to take into account additional requirements about the security of your processing – and these also apply to data processors.
- ✓ You can consider the state of the art and costs of implementation when deciding what measures to take – but they must be appropriate both to your circumstances and the risk your processing poses.
- ✓ Where appropriate, you should look to use measures such as pseudonymisation and encryption.
- ✓ Your measures must ensure the 'confidentiality, integrity and availability' of your systems and services and the personal data you process within them.
- ✓ The measures must also enable you to restore access and availability to personal data in a timely manner in the event of a physical or technical incident.
- ✓ You also need to ensure that you have appropriate processes in place to test the effectiveness of your measures and undertake any required improvements.

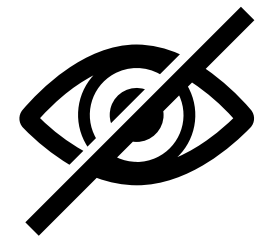




INTEGRITY AND CONFIDENTIALITY (SECURITY)

Checklist

- ☐ We undertake an analysis of the risks presented by our processing and use this to assess the appropriate level of security we need to put in place.
- ☐ When deciding what measures to implement, we take account of the state of the art and costs of implementation.
- ☐ We have an information security policy (or equivalent) and take steps to make sure the policy is implemented.
- ☐ Where necessary, we have additional policies and ensure that controls are in place to enforce them.
- ☐ We make sure that we regularly review our information security policies and measures and, where necessary, improve them.
- ☐ We have assessed what we need to do by considering the security outcomes we want to achieve.
- ☐ We have put in place basic technical controls such as those specified by established frameworks like Cyber Essentials.
- ☐ We understand that we may also need to put other technical measures in place depending on our circumstances and the type of personal data we process.
- ☐ We use encryption and/or pseudonymisation where it is appropriate to do so.
- ☐ We understand the requirements of confidentiality, integrity and availability for the personal data we process.
- ☐ We make sure that we can restore access to personal data in the event of any incidents, such as by establishing an appropriate backup process.
- ☐ We conduct regular testing and reviews of our measures to ensure they remain effective, and act on the results of those tests where they highlight areas for improvement.
- ☐ Where appropriate, we implement measures that adhere to an approved code of conduct or certification mechanism.
- ☐ We ensure that any data processor we use also implements appropriate technical and organisational measures.

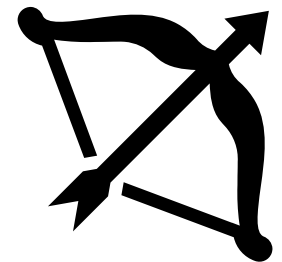




ACCOUNTABILITY PRINCIPLE (AND GOVERNANCE)

The accountability principle requires you to take responsibility for what you do with personal data and how you comply with the other principles. You must have appropriate measures and records in place to be able to demonstrate your compliance.

- ✓ Accountability is one of the data protection principles - it makes you responsible for complying with the GDPR and says that you must be able to demonstrate your compliance.
- ✓ You need to put in place appropriate technical and organisational measures to meet the requirements of accountability.
- ✓ There are a number of measures that you can, and in some cases must, take including:
 - adopting and implementing data protection policies;
 - taking a 'data protection by design and default' approach;
 - putting written contracts in place with organisations that process personal data on your behalf;
 - maintaining documentation of your processing activities;
 - implementing appropriate security measures;
 - recording and, where necessary, reporting personal data breaches;
 - carrying out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals' interests;
 - appointing a data protection officer; and
 - adhering to relevant codes of conduct and signing up to certification schemes.
- ✓ Accountability obligations are ongoing. You must review and, where necessary, update the measures you put in place.
- ✓ If you implement a privacy management framework this can help you embed your accountability measures and create a culture of privacy across your organisation.
- ✓ Being accountable can help you to build trust with individuals and may help you mitigate enforcement action.





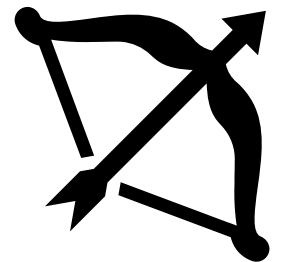
ACCOUNTABILITY PRINCIPLE (AND GOVERNANCE)

Checklist

- ☐ We take responsibility for complying with the GDPR, at the highest management level and throughout our organisation.
- ☐ We keep evidence of the steps we take to comply with the GDPR.

We put in place appropriate technical and organisational measures, such as:

- ☐ adopting and implementing data protection policies (where proportionate);
- ☐ taking a 'data protection by design and default' approach - putting appropriate data protection measures in place throughout the entire lifecycle of our processing operations;
- ☐ putting written contracts in place with organisations that process personal data on our behalf;
- ☐ maintaining documentation of our processing activities;
- ☐ implementing appropriate security measures;
- ☐ recording and, where necessary, reporting personal data breaches;
- ☐ carrying out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals' interests;
- ☐ appointing a data protection officer (where necessary); and
- ☐ adhering to relevant codes of conduct and signing up to certification schemes (where possible).
- ☐ We review and update our accountability measures at appropriate intervals.



Thank you!



The project is co-financed with the support of the European Union's Justice programme