GDPR Toolkit

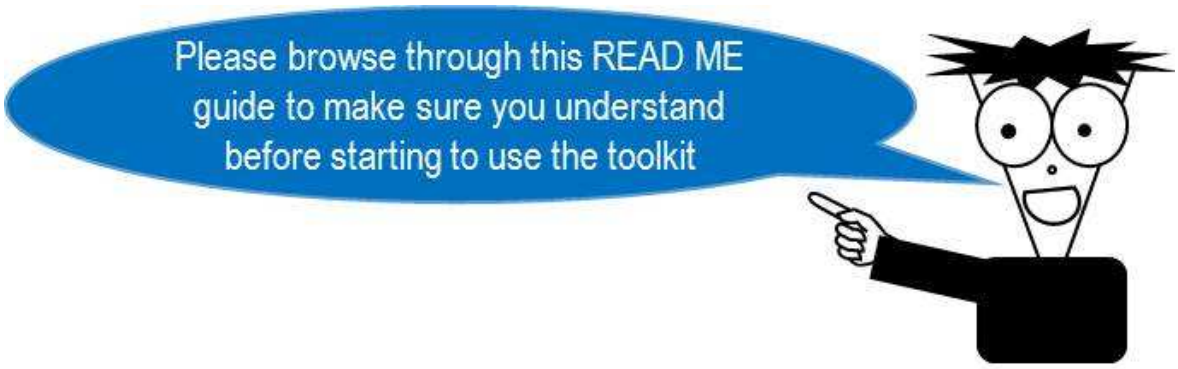
READ ME GUIDE

READ ME GUIDE FOR GDPR-TOOLKIT

WELCOME

This GDPR-Toolkit has been developed following work with a number of different organisations and represents a collection of policies, procedures, guidance and forms which I have found to be useful.

Contents



PRINCIPLES

This is a DIY ”self-assembly-kit” which contains policies, procedures, guides, and forms. Each organisation will be different and you will need to add, amend, or delete in order to reflect your people, processes and technologies as well as the data you hold and the jurisdiction(s) you operate in. Please read this guide to help navigate around the GDPR-Toolkit and identify what you need to do for your organisation.

If DIY isn’t for you, that’s OK. I’m rubbish at electrical work, plumbing or carpentry. Call an expert. There are many out there and data protection is too important for you, your organisation and the people who trust you with their data for you to get it wrong.

GDPRToolkit

1. TOOLKIT CONTENTS

There are presently 18 elements to the GDPRToolkit. I have outlined the core components of the GDPRToolkit below which will hopefully help make sense of it.

Let's start by explaining what is GDPR - GDPR is General Data Protection Regulation and is used as a generic term reflecting the new wave of Data Protection Regulation happening across Europe, including UK, Jersey and Guernsey.

For all other terms there is a glossary included.

It may be useful to think of GDPR in terms of policy, process, procedures and other documents you should have, as well as behaviours, tasks and actions that you should do.

Step	Task	Document
1	The first step is to identify someone to be the data champion to co-ordinate all the work Most organisations will not need a formal DPO, but there is merit in nominating someone to be the "data-champion" to help manage and co-ordinate the work that needs doing.	**Data protection officer (DPO) job description.**
2	The next step you need to do is understand what data you have got. Some may be on you PC, on a network, in the cloud, shared with colleagues or a friend. As a result some may be in Jersey, some may be in the UK and some maybe "anywhere". You need to know where your data is and what control you have over it.	**Mapping policy, procedure and forms**
3	The next step is to develop a data protection policy about the roles, goals and controls to protect the data.	**Data Protection Policy**
4	The next step is to consider what data needs to be kept or deleted	**Retention of records procedure**
5	The next step is to consider information security and the people, process and technology safeguards over data	**Information security policy**
6	The next step is to consider any particular risks and actions with the remaining data	**Data protection impact assessment procedure**
7	Be clear on when to outsource data and the due diligence needed and controls demanded	**International data transfer policy, procedure and forms**
8	Then consider the processor-controller or other controls to be applied to anyone who shares data	**Processor-Controller Agreement**
9	When you know about the data, the policies and procedures and the suppliers you can provide a Privacy Notice Your privacy notice need to tell people what data you hold	**Privacy policy, procedure and notice**

	on them and why. This notice for customers might be on a website or broaches, the notice for staff might be in the Employee Handbook, the notice for suppliers might be in their contract. There are many places and method let people know what data you hold on them and why..	
10	When you know everything for a Privacy Notice you can also satisfy a subject access request	**Subject access request form and procedure**
11	When you know everything for a subject access request you can also do a Breach Notification	**Breach policy and procedure**
15	When you have clarity on policy and procedures ensure staff understand and follow them	**Training policy and form**
16	When you have clarity on policy and procedures ensure they are being followed	**Audit checklist for compliance**
17	If something goes wrong with the above you may need to manage complaints	**Complaints procedure**
18	In some cases they may be entitled to take back their data or move it somewhere else	**Data portability policy, procedure and forms**

Note that some of these separate elements can be combined. For example the **Data Protection Policy** and the **Information Security Policy**, and possibly the **Retention Of Records Procedure** might all be elements in the **Staff Handbook**.

In a similar way, the **Privacy policy, procedure and notice** and the **Subject access request form and procedure** might both be elements in a **customer contract.**

Moreover some elements may simply not apply, for example if all your data and processing is in Jersey you may not need **International data transfer policy, procedure and forms.**

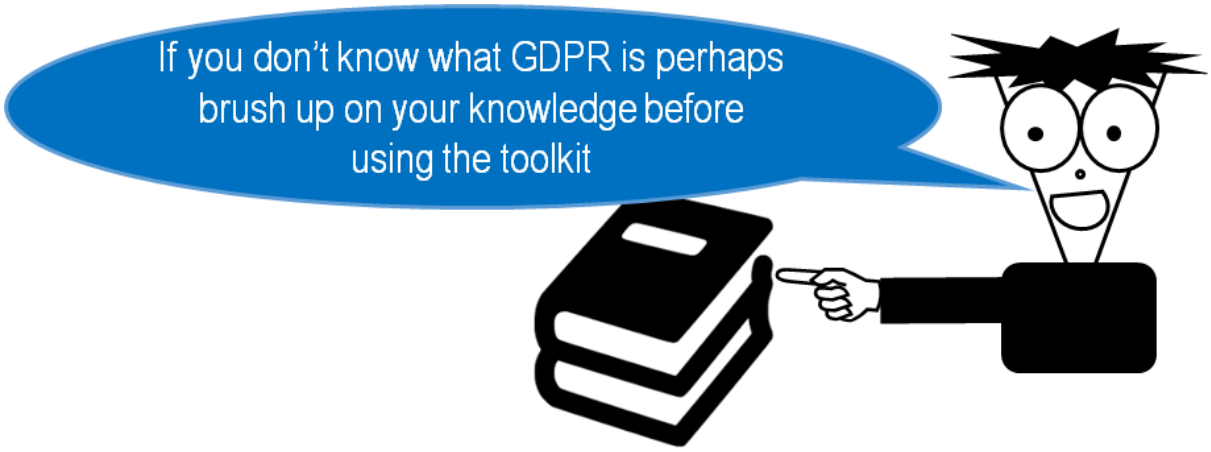
Also not all organisations need a Data Protection Officer so you may not need a **Data protection officer (DPO) job description**

The key point is that this a toolkit you don't need to use every tool for every job, just pick what is right for what you need to do, customise it where necessary and seek further advice if in doubt.

2. WHAT SHOULD I DO FIRST

The GDPRToolkit been developed following presentations to 160 charities, 10 businesses and 60 sports clubs and assumes that you have a basic understanding of GDPR and are now looking for a toolkit of policies, processes, procedures and forms to help you organisation comply.

I do provide training and would be happy to help if you need support. There are many lawyers, consultancies and training companies offering training for GDPR.

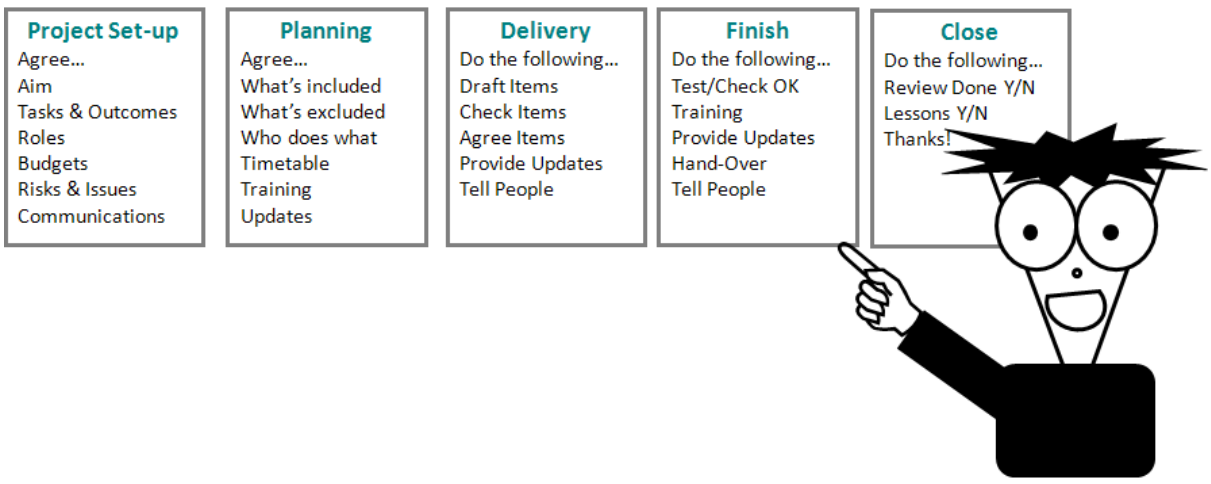


For self-help I recommend the following on-line resources

Video https://thinkgdpr.org/
Guidance https://thinkgdpr.org/resources/

3. MANAGING YOUR GDPR PROJECT

This is a toolkit, not a guide on Project Management. However there a few simple things to consider if you end-up being the person who needs to coordinate all of this and you need to think about organising other people as well as worrying about budget, schedule, and getting things done right.



If you want training on or support with Project Management please get in touch. We are very experienced and very successful at Project Management.

4. USING THE GDPR TOOLKIT

I have been asked if it can be made simpler.

In truth for a one-person organisation holding the address list of 10 people who come to their events could be as simple as making sure people agree that you can have their data and keeping the data safe and secure in a locked cabinet or protected computer – job done!

The problem is that I don't know if the GDPRToolkit is being downloaded by a one-person organisation or a large organisation with many employees and lots of sensitive data in many places. So the GDPRToolkit must be treated as a template and people will have to add, amend or delete the sections that apply to them.

5. BONUS ITEM: ADDITIONAL GUIDANCE

As well as the documents and templates the GDPRToolkit include some useful guidance from the regulator(s). This is publically available and free to share with anyone.

This Includes
Copies of the Jersey Legislation
Copies of the Jersey Guidance
Copies of the Guernsey Guidance
Copies of the UK Data-Mapping Templates

Sources
UK ICO regulatory website https://ico.org.uk/
Jersey OIC regulatory new website www.OICJersey.org
Jersey OIC regulatory old website https://www.dataci.org/
Guernsey ICO regulatory website https://dataci.gg/

ICO = Information Commissioner Office
OIC = Office of Information Commissioner

6. GUIDANCE FROM THE REGULATOR(S).

I have been careful to make reference to the law and the guidance from the regulator(s) so that for each element in the GDPRToolkit you can check exactly what the regulator(s) say and make your own decisions about how to customise the documents and templates to suit your people, processes and technologies as well as the data you hold and the jurisdiction(s) you operate in.

At least 90% of UK, EU, Jersey and Guernsey GDPR is the same – the whole idea is to create a standard approach across the whole of Europe. There are some modest differences (for example in relation to Jersey's treatment of Trusts) but on the whole the GDPRToolkit addresses all the key issues.

Currently the front-runner on regulations and guidance is the UK ICO, but both Jersey and Guernsey are planning to release guidance relating to their approach to GDPR. I can add or update with Jersey and Guernsey where necessary.

I have met with the regulator(s) many times during the development of this toolkit and I can say that they are there to help people. They are more interested in helping people do the right thing than punishing people. However the regulator(s) have a range of enforcement tools for organisations that are wilfully negligent or reckless.

If there is a factor that you are not certain about, or value guidance on, just ask.

If you do need to seek legal or regulatory advice on a point of detail at least the GDPRToolkit will have got you 90% there, which is a pretty good starting point.

7. SUPPORT FOR THE GDPR TOOLKIT

For those organisations without the resources, skills or experience I am willing to help customise to meet their particular needs. If a bunch of similar organisations want to work together to share ideas and costs I would be happy do work within a team.

8. ALTERNATIVE TO THE GDPR TOOLKIT

The GDPRToolkit is just an option and if you prefer to create your own policies, procedures, guidance and templates I can thoroughly recommend the resources available on the ThinkGDPR website here.

https://thinkgdpr.org/resources/

9. DISCLAIMER

GDPR can be complicated and there are different laws in UK, EU, Jersey and Guernsey. Simply having Templates, Documents, Samples and Guidance does not make you compliant.

The reason for this disclaimer is that I cannot warrant or guarantee materials for every system or circumstance or jurisdiction and the client/user/recipient is obliged to review, test and where necessary customise or take advice to generally assert that they are satisfied before using this “live”.

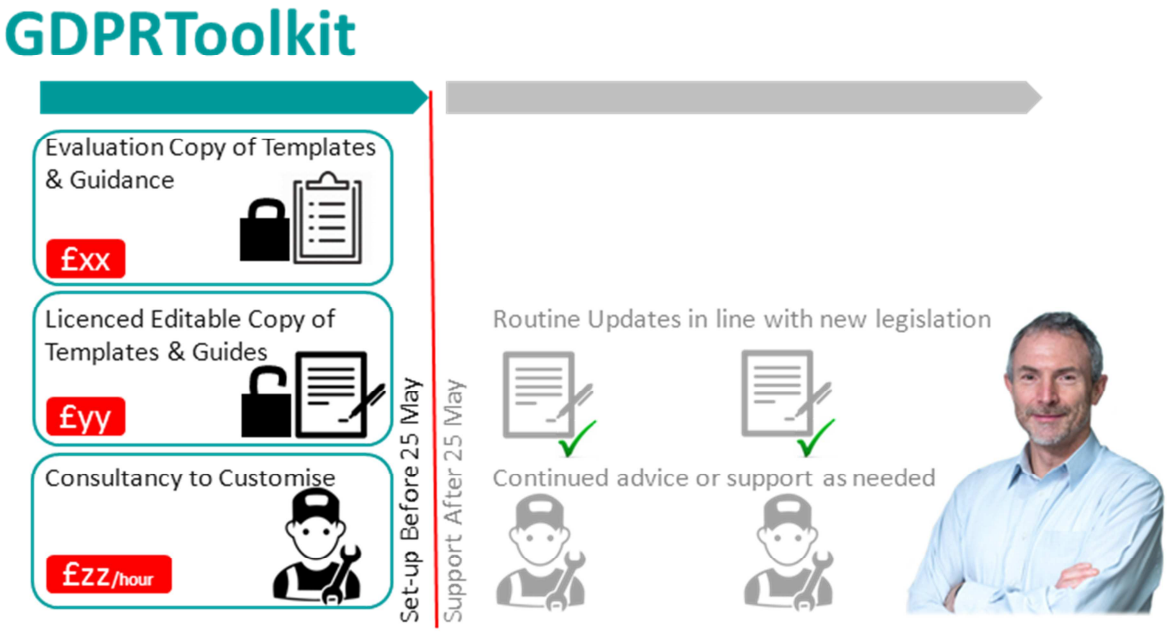
10. LICENCE FOR THE GDPR TOOLKIT

With the obvious exception of the published guidance of the regulator(s) [The Bonus Items] the GDPRToolkit is subject to a Creative Commons License and has restrictions and is subject to copyright and disclaimers.

1. There is a read-only evaluation copy which ostensibly acts as a guide and practical to-do list for GDPR with samples of the documents and suggestions for the actions you need to take.

2. There is a licenced read-edit copy which is licenced (meaning you cannot resell or share it with others without permission). This is fully customisable to meet your organisation and inevitably will need to be edited to reflect your people, processes and technologies as well as the data you hold and the jurisdiction(s) you operate in.

For those organisations without the resources, skills or experience I am willing to help customise to meet their particular needs. If a bunch of similar organisations want to work together to share ideas and costs I would be happy do work within a team.



For those that need it I can offer an update service which will provide bulletins on new regulations and guidance. Currently the front-runner on regulations and guidance is the UK ICO, but both Jersey and Guernsey are planning to release guidance relating to their approach to GDPR.

I also offer a consultancy/advisory check-up service on a retainer to offer support or advice or simply to be a someone to bounce ideas off.

11. CONTACT

Tim HJ Rogers
Mob 447797762051 timhjrogers@gmail.com
Skype timhjrogers Twitter @AdaptCCompany
Adapt Consulting CompanyConsult, CoCreate, Deliver
Business Analysis – Projects – Processes – Programmes
Website http://www.adaptconsultingcompany.com
Find us on Facebook@AdaptConsultingCI
To access our disclaimer and T&Cs please visit our webpage
http://www.adaptconsultingcompany.com/terms/

12. GLOSSARY

Let's start with the GDPR - GDPR is General Data Protection Regulation and is used as a generic term reflecting the new wave of Data Protection Regulation happening across Europe, including UK, Jersey and Guernsey.

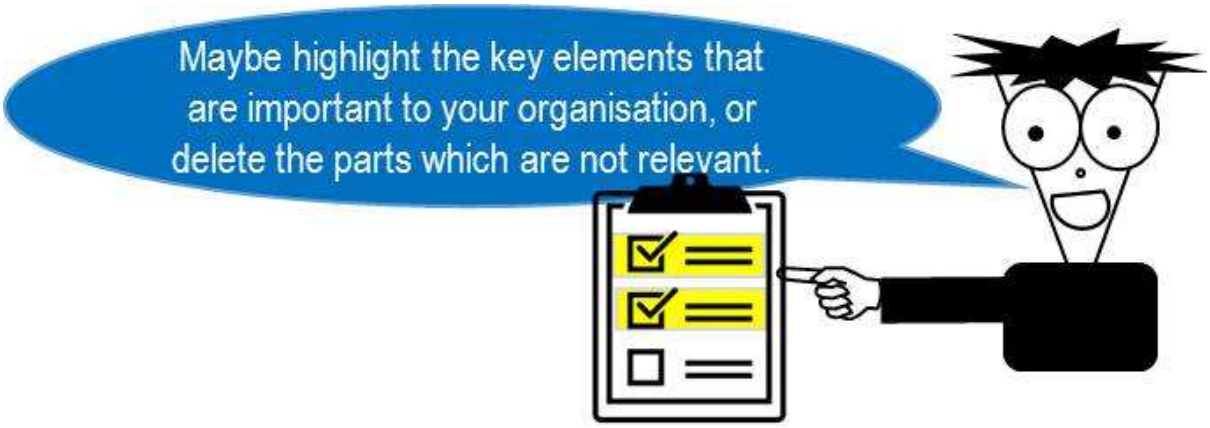
GDPRToolkit

Not all these terms are used in the GDPRToolkit, nonetheless it is useful to know them because these are core elements of GDPR and feature in the law and regulatory guidance.

Since the GDPRToolkit may be used by a small one-person charity organisation or a large multi-national business with offices in UK, EU and elsewhere it is important to include all the terms in order for organisations to identify any special considerations or factors including those not covered in the GDPRToolkit.

Sources

UK regulatory website https://ico.org.uk/
Jersey regulatory new website www.OICJersey.org
Jersey regulatory old website https://www.dataci.org/
Guernsey regulatory website https://dataci.gg/



Accountability Principle	The Controller has responsibility for and must be able to demonstrate compliance with all the principles listed above.
Accuracy Principle	Personal data must be accurate and kept up to date and every reasonable step must be taken to ensure that inaccurate personal data is erased or rectified without delay.
Binding Corporate Rules (BCRs)	a set of binding rules put in place to allow multinational companies and organisations to transfer personal data that they control from the EU to their affiliates outside the EU (but within the organisation)
Biometric Data	any personal data relating to the physical, physiological, or behavioral characteristics of an individual which allows their unique identification
Consent	freely given, specific, informed and explicit consent by statement or action signifying agreement to the processing of their personal data
Data Concerning Health	any personal data related to the physical or mental health of an individual or the provision of health services to them
Data Controller	is the natural or legal person, public authority, agency or other body which alone, or jointly with others, determines the purpose and means of the processing of personal data; where the purposes and means of processing are determined by European Union law or Member State law, the controller or the specific criteria for his nomination may be designated by European Union law or by Member State law.
Data Erasure	also known as the Right to be Forgotten, it entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of

	the data, and potentially have third parties cease processing of the data
Data Portability	the requirement for controllers to provide the data subject with a copy of his or her data in a format that allows for easy use with another controller (more info here)
Data Processing	any operation or set of operations performed upon personal data, or sets of it, be it by automated systems or not. Examples of data processing explicitly listed in the text of the GDPR are: collection, recording, organising, structuring, storing, adapting, altering, retrieving, consulting, using, disclosing by transmission, disseminating or otherwise making available, aligning or combining, restricting, erasure or destruction.
Data Processor	a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
Data Protection Authority	national authorities tasked with the protection of data and privacy as well as monitoring and enforcement of the data protection regulations within the Union
Data Protection Officer	an expert on data privacy who works independently to ensure that an entity is adhering to the policies and procedures set forth in the GDPR (more info here)
Data Subject	a natural person whose personal data is processed by a controller or processor
Delegated Acts	non-legislative acts enacted in order to supplement existing legislation and provide criteria or clarity
Derogation	an exemption from a law
Directive	a legislative act that sets out a goal that all EU countries must achieve through their own national laws
Encrypted Data	personal data that is protected through technological measures to ensure that the data is only accessible/readable by those with specified access
Enterprise	any entity engaged in economic activity, regardless of legal form, including persons, partnerships, associations, etc.
Fairness Principle	Fairness is achieved when the Data Controller has put in place working procedures for the Data Subject to exercise in an effective manner the following rights: 1. Right of access to the data (to know what data is held about the individual). 2. Right to rectification of the data. 3. Right to erasure of the data (to be forgotten). 4. Right to restriction of processing. 5. Right to data portability (to be given personal data in a structured and commonly used and machine-readable format and transmit such data to another controller). 6. Right to object to the processing of personal data, including profiling. 7. Right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects or significantly affects him/her.
Filing System	any specific set of personal data that is accessible according to specific criteria, or able to be queried
Genetic Data	data concerning the characteristics of an individual which are inherited or acquired which give unique information about the health or physiology of the individual
Group of Undertakings	a controlling undertaking and its controlled undertakings
Integrity and	Personal data must be processed using appropriate technical and

Confidentiality Principles	organisational security measures, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.
Legality Principle	Personal data must be processed only on the basis of one of the legal grounds specified by the GDPR. In practice, this means that for any personal data element processed, an organisation must be able to indicate on which of the following list of grounds it is processing it: 1. Individual's own consent. 2. Contract with the individual. 3. Complying with an existing legal obligation. 4. Necessary to protect the vital interests of a person. 5. Necessary for a task in the public interest or in the exercise of public authority. 6. Necessary in the pursuit of the legitimate interest of the organisation or a third party.
Main Establishment	the place within the Union that the main decisions surrounding data processing are made; with regard to the processor
Minimisation Principle	Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.
Personal Data	any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, by reference to an identifier: ID number, location data, online identifier, or factors specific to physical, physiological, genetic, mental, economic, cultural or social identity of that person.
Personal Data Breach	breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
Principles	All of the fundamental principles in the GDPR are further "translated" into detailed rights for the individual and corresponding obligations for the organisation. Additionally all of the principles are reinforced with the overarching Accountability principle: this means that organisations (Data Controllers) not only must follow each Data Protection principle, but must also be able to prove how they are putting each into practice.
Privacy by Design	a principle that calls for the inclusion of data protection from the onset of the designing of systems, rather than an addition
Privacy Impact Assessment	a tool used to identify and reduce the privacy risks of entities by analysing the personal data that are processed and the policies in place to protect the data
Processing	any operation performed on personal data, whether or not by automated means, including collection, use, recording, etc.
Profiling	any form of automated processing of personal data using it to evaluate, analyse or predict certain personal aspects of a natural person. Examples of profiling explicitly listed in the text of the GDPR are: performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
Pseudonymisation	the processing of personal data so that it can no longer be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and technical and organisational measures are used to ensure non-attribution to an identified or identifiable person.
Purpose Limitation Principle	Personal data must be collected for specified, explicit, legitimate purposes and not further processed in a way incompatible with those purposes. Public

	interest archiving, scientific, historical, statistical research are deemed to be compatible with the initial purpose.
Recipient	entity to which the personal data are disclosed
Regulation	a binding legislative act that must be applied in its entirety across the Union
Representative	any person in the Union explicitly designated by the controller to be addressed by the supervisory authorities
Right to Access	also known as Subject Access Right, it entitles the data subject to have access to and information about the personal data that a controller has concerning them
Right to be Forgotten	also known as Data Erasure, it entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties cease processing of the data
Storage Limitation Principle	Personal data must be kept in a form which permits identification of data subjects for no longer than necessary for the processing purposes. Data may be stored for longer periods only for public interest archiving, scientific, historical or statistical research purposes.
Subject Access Right	also known as the Right to Access, it entitles the data subject to have access to and information about the personal data that a controller has concerning them
Supervisory Authority	a public authority which is established by a member state in accordance with article 46
Transparency Principle	Any information the data controller (organisation) gives to the data subject (individual) about its data processing practices must be concise, transparent, intelligible and in easily accessible form; must be provided at the latest within one month, in writing. The data controller can only refuse if it can demonstrate that it is not in a position to identify the data subject. If the data controller does not take action on the request, it must inform the data subject at the latest within a month of the reasons for not taking action and of the possibility of lodging a complaint to a supervisory authority and of seeking a judicial remedy. Information shall be free of charge, unless the requests are unfounded, excessive or repetitive, in which case the controller may charge an administrative fee but bears the burden of proving the unfounded or excessive character of the request.
Trilogues	informal negotiations between the European Commission, the European Parliament, and the Council of the European Union usually held following the first readings of proposed legislation in order to more quickly agree to a compromise text to be adopted.