

May 2018

Presentation Summary



General
Data Protection
Regulation (GDPR)
It's time to comply

The new Global Data Privacy Regulation will first become effective on **May 25th 2018 in Europe**.

This stronger rules on data protection means citizens have more control on their personal data. That forces companies that have European consumer data to review their usage of the data, be transparent on usage of that data, improve personalisation and build trust with consumer.

We all see impact of personal data usage and trust to big companies like Facebook.

This presentation will :

- Share key rules and changes with GDPR
- Key new role and obligations
- Impact outside of Europe like US-EU Privacy Shield
- Marketing key benefits
- First steps and how to become compliant

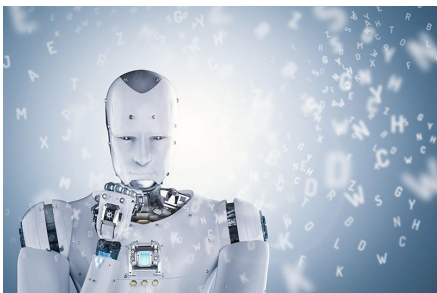
Introducing myself



More than 25 years in Information technology where last 20 were focused on Digital strategy, roadmap and solution design/ implementation.

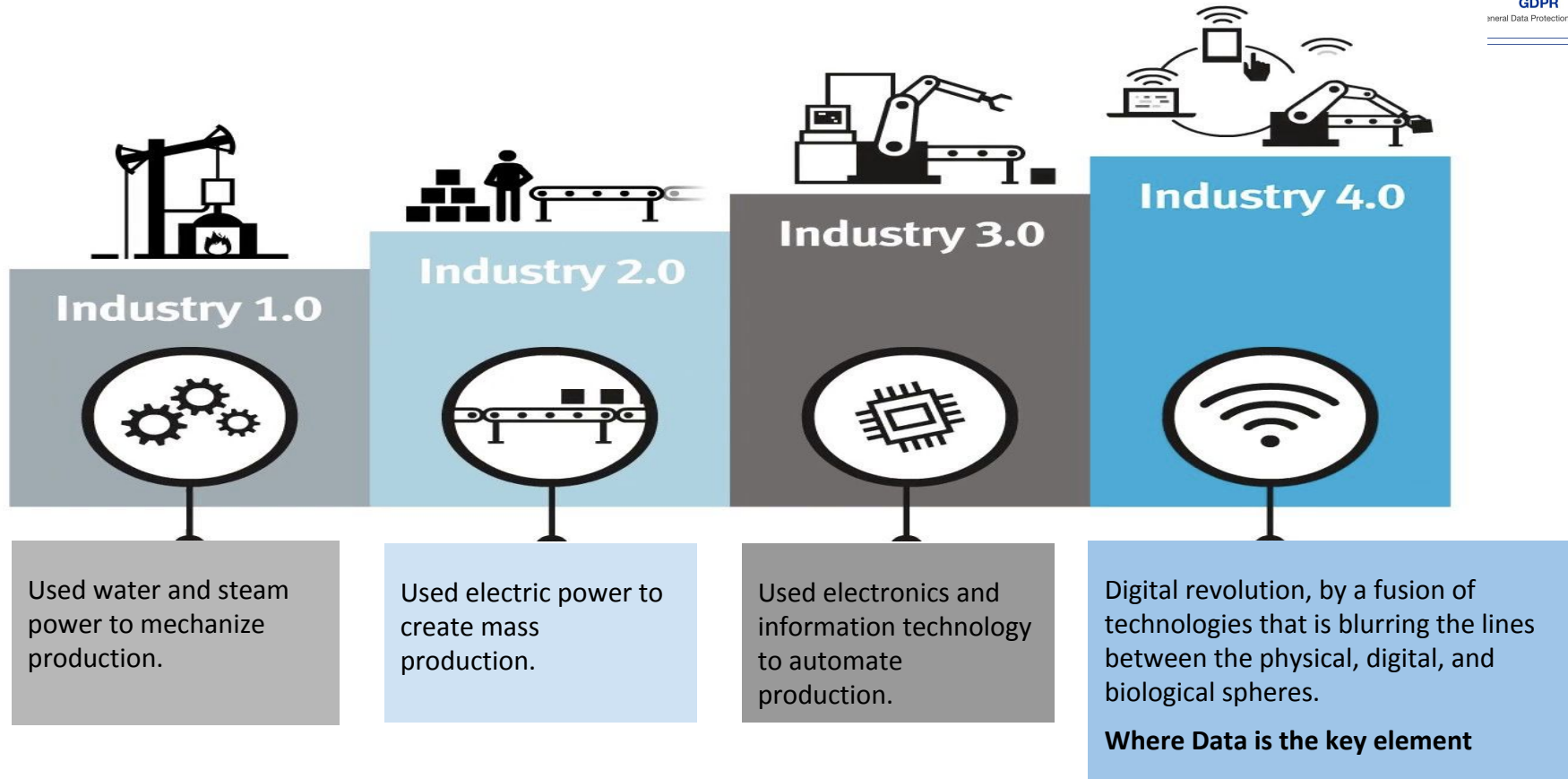
Among key companies, worked for IBM Global Services global team and last Whirlpool Corporate, where I was Sr Manager IT for EMEA digital Ecosystem.

There I spend 1 year on GDPR, to understand impact, secure team, support Funding request, select proper tools and implement privacy by design with Lawyers, Marketing and IT colleagues.



Digital continue to evolve every year, the new right to data privacy will be as important as mobile phone launch in 1956 to smartphone with large capacity touchscreen launched in 2007.

4th Industrial revolution is now



Data Protection (GDPR) is almost active



Data protection

Better rules for small business

Stronger rules on data protection from 25 May 2018 mean citizens have more control over their data and business benefits from a level playing field. One set of rules for all companies operating in the EU, wherever they are based. Find out what this means for your SME.



Origins and historical context of Data protection



10 Dec 1948

- Human Rights Declaration adopted by General Assembly of the United Nations

1950

- In Rome the Council of Europe get individual states to sign the European Convention on Human Rights (ECHR)

3 Sept 1953

- ECHR entered into force

1968

- Council of Europe did a publication of Recommendation 509 on Human Rights and Modern and Scientific Technological Developments.

1973 - 1974

- The Council of Europe initial work with Resolutions 73/22 and 74/29, that established principles for the protection of personal data

23 Sep 1980

- OECD Guidelines on Protection of Privacy and Transborder Flows of Personal Data (cooperation with Council of Europe & European Community)

28 Jan 1981

- Convention 108 (Convention for the protection of Individuals with Regard to Automatic Processing of Personal Data) signed member states of Council Europe

24 Oct 1995

- Directive 95/46/EC is adopted (European data protection directive)

GDPR History



The History of the

GENERAL DATA PROTECTION REGULATION (GDPR)

1984

Data Protection Act passed
United Kingdom



1995

Data Protection Directive passed
European Union

2000

International Safe Harbor
Privacy Principles
established



1998

Data Protection
Act 1998 passed
United Kingdom



2012

European Commission
announces its plan to
develop the GDPR



2015

International Safe Harbor
Privacy Principles
overturned



MAY 25
2018

GDPR takes effect

GDPR

APRIL 14
2016

GDPR is approved
by EU Parliament

FEBRUARY 2
2016

EU-US Privacy Shield replaces
the International Safe Harbor
Privacy Principles

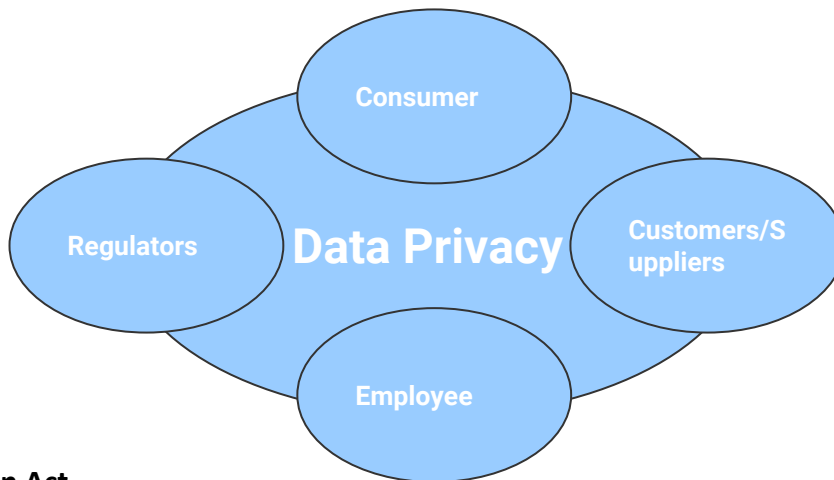
1984

2018

GDPR High Level view



- 1 Improve Privacy Compliance
- 2 Protect Brand
- 3 Build Trust



GDPR vs 1995 EU Directive / 1998 UK Data protection Act

- Heavy Fines up to **800 Million** from Regulators (CNIL, AEPD, ICO, BDSG)
- Data Portability
- Notification of breach internal (**72 hours**) to share and take action
- Right to access/erasure
- Accountability principle
- Mandatory Privacy Impact Assessment (privacy by design)
- Current data breaches each year much higher- 736 million in 2015

Unlike many regulatory requirements, the guidelines for penalties have been set high enough that ignoring GDPR and paying the fines will not be an acceptable strategy.

Non compliance impact

Your local Data Protection Authority monitors compliance; their work is coordinated at EU-level.
The cost of falling foul of the rules can be high.



What is Personal Data?

- 
-  Name
 -  Address
 -  Localisation
 -  Online identifier
 -  Health information
 -  Income
 -  Cultural profile
 -  and more

**COLLECT
STORE
USE
DATA?**

You have to abide by the rules.

Process data for other
companies?
This is for you too.

Article 4(1):

1. any information
2. relating to
3. an identified or identifiable
4. natural person



Special category of personal data



In the category of **special or sensitive personal data** addressed in **Article 9 GDPR**, one can find information revealing

1. racial or ethnic origin,
2. political opinions,
3. religious or philosophical beliefs,
4. trade union membership,
5. genetic data,
6. biometric data used to uniquely identify natural persons,
7. health data,
8. data concerning individuals' sex life,
9. sexual orientation.

Article 9(1): Special categories of personal data

'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'.

Processing of personal data : Exceptions (Article 9)



Explicit Consent



Political, philosophical
and religious purposes

In the context of employment

Vital interests

Establishment, exercise or
defence of legal claims

Substantial public interest

Research or statistical purposes

Preventive or occupational
medicine

Public Health

GDPR Processing Principles (Article 5)



GDPR processing principles

Lawfulness, fairness and transparency of processing

Purpose limitation

Data minimisation and proportionality

Data quality and accuracy

Storage limitation

Integrity and confidentiality

Accountability

1) Lawfulness, fairness and transparency.

2) Purpose limitation.

3) Data minimisation.

4) Accuracy

5) Storage limitation

6) Integrity and confidentiality

7) Accountability

GDPR Key new role and obligations



Data subject

Data controller

Data processor

Supervisory
authority

Obligations of Controller and Processor



Controller Records

- Name and contact information of the controller and DPO
- Categories of data subjects, personal data and recipients of that data
- International data transfers being made and the measure put in place to ensure they are lawful
- How long the personal data is being retained and the timeline for deleting that data
- A general description of technical and organisational security measures that have been implemented



Processor Records

- Name and contact information of the processor, the controller and DPO
- Categories of processing carried out on behalf of the controller
- International data transfers being made and the measure put in place to ensure they are lawful
- None (on data retention or deletion)
- A general description of technical and organisational security measures that have been implemented

Obligations of controllers and processors toward DPO



What circumstances require a DPO?

Article 37




The controller is a public authority

Core activities include regular and systematic monitoring on a **large scale**

Core activities consist of **large-scale** processing of special categories

- Provide support to the DPO , including resources to help carry out tasks
- Provide Access to personal data and processing operations
- Help the DPO maintain expert knowledge of topics and issues related to personal data protection
- Ensure the DPO acts completely independently and does not receive instructions from anyone except the supervisory authority
- Ensure the DPO is not dismissed or penalised for performing his or her tasks
- Ensure the DPO is not put in a situation that is a conflict of interest
- Ensure that the DPO reports to the highest levels of management. This is important because it will prevent messages from getting attenuated before reaching management

When must Controller contact Supervisory Authority



When Data protection impact assessment indicates high risk to data subjects that are not mitigated, and must include:

- Responsibilities of the controllers and processors
- Purposes and means of the processing
- Measures and safeguards
- Contact details of the DPO

Supervisor Authority reply:

- Will provide answer within 8 weeks
- May block the process for more information
- May allow additional 6 weeks for complex process

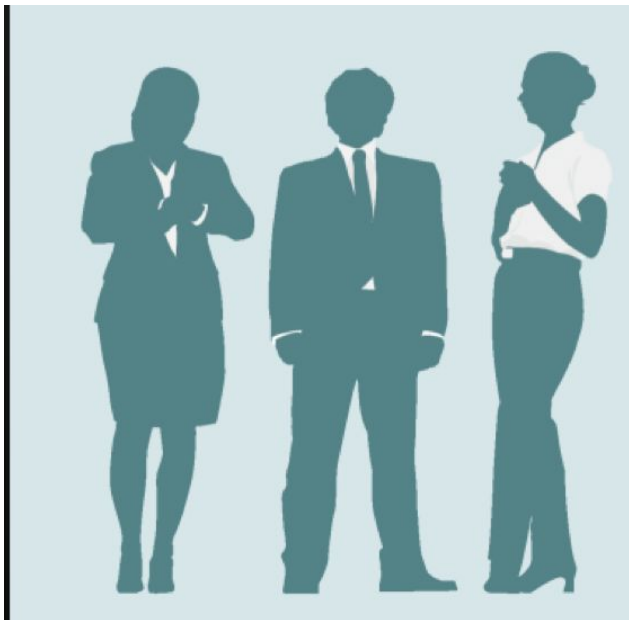
Supervisory authorities: Mechanisms



Mechanisms

Cooperation	Cooperation between the lead supervisory authority and other concerned supervisory authority to reach consensus
Mutual assistance	Provision of relevant information between supervisory authorities
Joint operations	Joint Investigations and enforcement measure of controllers or processors in several member states or of data subjects in >1 member state
Consistency mechanism	Specific collaborative process between SA, the Commission and EDPB for adopting certain measures and ensuring consistent GDPR application
Dispute resolution	Dispute a decision and the issuance of binding decisions
Urgency procedure	Procedure for the immediate adoption of provisional measures within a member state

European data protection Board (EDPB)



Article 29
Working Party



European Data
Protection Board

31 representatives

28 active members

EDPB Chair

European Data
Protection
Supervisor (EDPS)

Representatives of
the Commission

Key activities of EDPB:

- Monitor for correct GDPR application
- Oversee the consistency mechanism
- Issue guidance and advice to the Commission
- Preside over the dispute-resolution process

Impact outside of Europe like US-EU Privacy Shield



Cross-border data transfers options

The landscape of cross-border data transfers in order:

1. Adequacy decisions
2. Appropriate safeguards
3. Derogations

Controller obligation to notify data subjects

Existence or absence of an adequacy decision

Intent to transfer personal data internationally

Safeguards



Cross-border data transfers: Adequacy Decisions



- Indicates there is an adequate level of data protection for a country. Under GDPR, adequacy has broadened to include territories, sectors (for example regulated financial or healthcare sectors) and international organisations
- The European Commission makes adequacy decisions. Under GDPR, adequacy decisions are to be reviewed every 4 years. If a country is found to have fallen short of the adequacy standards, then the decision can be repealed, suspended or amended. Already existing decisions will remain in force until amended, replaced or appealed.
- The GDPR sets out a number of factors that the European Commission must take into account when adopting adequacy decisions. The criteria and considerations used to make adequacy decisions includes:
 - Respect of the rules of law
 - Access to Justice
 - International human rights standards
 - general and sectoral law, and case law
 - Effective and enforceable rights for individuals, including effective administrative and judicial redress
 - Data protection rules, professional rules and security measures, including specific rules for onward transfers
 - Other international commitments and obligations

Cross-border data transfers :Adequacy decisions (countries)



Canada:

For data protected by PIPEDA,
applicable to commercial
organisations but not all forms of
personal data

United States:

For data protected by the EU-U.S.
Privacy Shield

Uruguay

Argentina



Faeroe Islands

Isle of Man

Guernsey and Jersey

Andorra

Switzerland

Israel

New Zealand

Cross-border data transfers: Appropriate Safeguards

(in the absence of adequacy decision)



Legal tools designed to ensure recipients of personal data, who are outside the EEA, are bound to continue to protect personal data to a European-like standard.

Binding Corporate rules	BCRs are designed to allow large multinational companies to adopt a policy suite with rules for handling personal data that are binding on the company. If those supervisory authorities sign off on the company, the company is considered free to transfer personal data within their organisation around the world. These internal and legally binding rules expressly confer enforceable rights of data subjects. Article 47 list minimum requirements of BCR. Note that there are different versions of BCRs for controllers and processors.
Standard contractual clauses	(model clause) Standard contractual clause are adopted by the Commission or by a national supervisory authority and then approved by the Commission. A company in the EEA that wants to send data to a company outside the EEA may use the appropriate standard. It is simply a standard form that is non-negotiable. Once signed, the company outside the EEA is considered safe.
Approved codes of conduct or certification mechanisms	Provisions within the GDPR encourage industries to create their own codes of conduct and certification mechanisms that will be reviewed by the European Data Protection Board. If approved, companies may adhere to them and be considered safe.
Ad Hoc contractual clauses	Ad hoc contractual clauses must have supervisory authority authorisation. They allow for individual tailoring to a company's needs. Provisions for such clauses may differ at the member state level.
Reliance on international agreements	Two countries may enter into an agreement between themselves to provide for the protection of personal data. For example, passenger name records(PNRs): If an individual flies from Europe to the U.S., the European authorities have to transfer information about the individual as a traveller over to the U.S. authorities.

OVERVIEW OF BCR UNDER GDPR

BCR APPROVAL TIMELINE (6 Months)



United States adequacy history



July 2000

- Safe Harbor is found adequate by the European Commission

Oct. 2015

- Safe Harbor is invalidated by the court of Justice of the EU as a result of the *Schrems v Data Protection Commissioner* case. The CJEU finds Safe Harbor to lack protection of fundamental rights 'essentially equivalent' to that in the EU. In particular, it says that national security, public interest and law enforcement have been placed above the Safe Harbor principles.

Feb. 2016

- Negotiations with the European Commission result in the EU-U.S. Privacy Shield agreement

July 2016

- The Commission formally approves the EU-U.S. Privacy Shield after review by the Article 29 Working Party, the European Parliament, the European Data Protection Supervisor and the Article 31 Committee, resulting in a revised text.

Aug. 2016

- Companies can sign up for the EU-U.S. Privacy Shield.

EU-U.S. Privacy Shield



Voluntary, self-certification programme

Most be unders U.S. Federal trade Commission
of other U.S. Authority

Requirements :

- Commit to adhere to the Privacy Shield Principles
- Publicise that commitment
- Implement the Principles
- Annually renew the certification
- Publicly disclose the privacy policy



Privacy Shield Principles to be implemented :

- Notice
- Choice
- Accountability for onward transfers and vendor agreements
- Security
- Data integrity and purpose limitation
- Access
- Resource, enforcement and liability

Notice:

Certain information must be provided to data subjects:

- The controller's identity
- Details about recourse mechanisms
- The ability to complain to authorities
- Where the Privacy Shield list is available online

Accountability for onward transfers and vendor agreements

All organisations now certifying are expected to be already in compliance with the Privacy Shield, including vendors agreements



Marketing key benefits with GDPR



Most company have:

- Collect several type of personal data from their consumers and employee
- Limited visibility on existing data processes
- Limited control on internal and partner personal data usage
- Limited tools to help manage personal data

Some key advantages:

- Learn more about consumer data privacy rights
- Retain their trust by being compliant
- Avoid GDPR fines
- Better usage of Consumer data



Key changes with Direct impact to Marketing



1. **Accountability and Data Governance:** take it seriously and demonstrate that you do so
2. **Privacy Policies:** more information to be given, but “easy to understand”, “concise” and in “clear and plain language”
3. **Consent:** will be harder to get and harder to rely on
4. **New rights:** right to be forgotten, portability guaranteed
5. **Profiling:** gets tougher, subject to greater focus and scrutiny (“explicit” consent required in certain circumstances)
6. **Privacy by Default or by Design**
7. **Mandatory Data Breach Notifications:** it is a “risk” assessment each time just in 72 hours
8. **Privacy Impact Assessment** for every new project or enhancement
9. **The “bottom line”:** new tougher fines of 4% of global turnover (for us that can be circa \$800M)
10. **Restricted International Data Transfers**

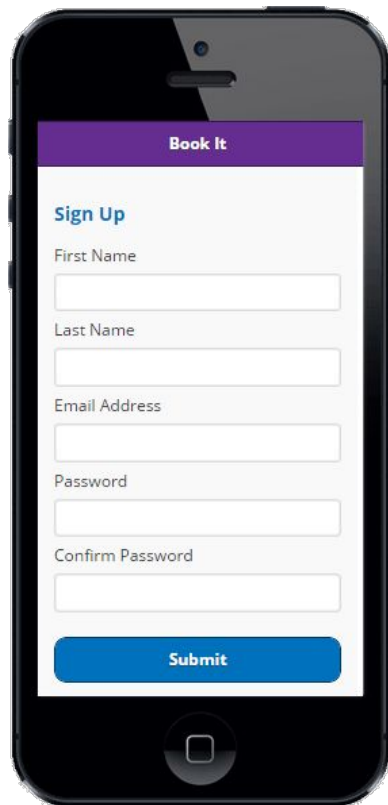
Update and refine Marketing Consent



*Consent is a **freely given, specific, informed** and **unambiguous** indication of the individual's wishes. The controller must **keep records so it can demonstrate** that consent has been given by the relevant individual.*

- **Plain language**
- **Separate**
- **Affirmative action**
- **Consent to all purposes**
- **No detriment**
- **No power imbalance**
- **Unbundled consent**
- **Not tied to contract**
- **Easy to withdraw**

When information directly collected (Article 13)



A smartphone screen showing a 'Sign Up' form. The form has a purple header with 'Book It' and a blue 'Sign Up' title. It contains input fields for First Name, Last Name, Email Address, Password, and Confirm Password, followed by a blue 'Submit' button.

From the controller :

- Identity and contact details
- Purpose and legal basis
- Recipients of personal data
- Intention to transfer data to a third party
- Legal basis for intended international transfer
- Legitimate interests
- Storage period
- Data subjects rights
- Statutory or contractual requirement
- Automated decision-making

Access to rectification



Normal process :

- The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her.
- Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

Complex change :

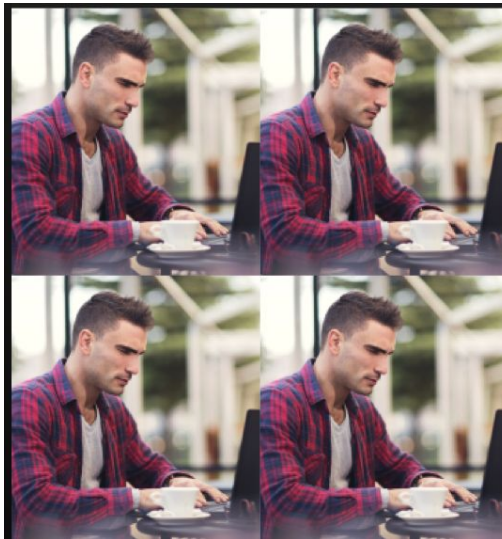
- Controller may have up to 2 additional months
- Must inform data subject for reason of the delay

Article 17: Right to be erase / Right to be forgotten

Erase



Forgotten



Potential difficulties:

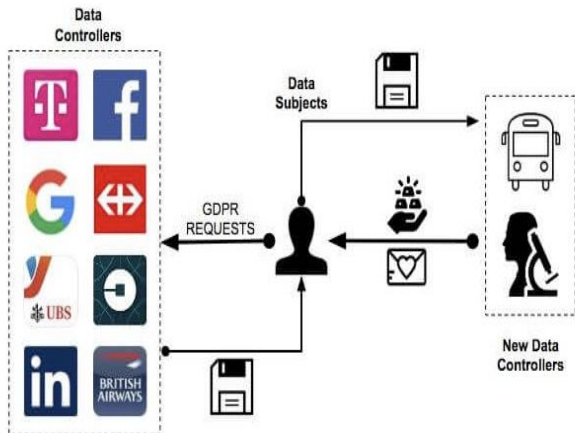
Determining all of the data's recipients

Informing all other controllers (which may result in increased exposure)

Objections from controllers based on the fundamental right to freedom of expression and information

Data portability (Article 20)

Portability rights



- The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.
- It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.
- Some organisations in the UK already offer data portability through the midata and similar initiatives which allow individuals to view, access and use their personal consumption and transaction data in a way that is portable and safe.
- It enables consumers to take advantage of applications and services which can use this data to find them a better deal, or help them understand their spending habits.

Article 21: Right to Object

The controller shall no longer process the personal data **unless the controller demonstrates** compelling **legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.**

Direct marketing:

A data subject has the right to be object at any time to the processing of his or her personal data of direct marketing purposes. This right is absolute and should cause the controller to cease processing. This right includes profiling



Research or statistical purpose:

A data subject may object to processing for scientific or historical research purposes or statistical purposes, on grounds relating to his or her particular situation. This right is overridden if the processing is necessary for the performance of a task carried out in the public interest.

Public interest or legitimate interests:

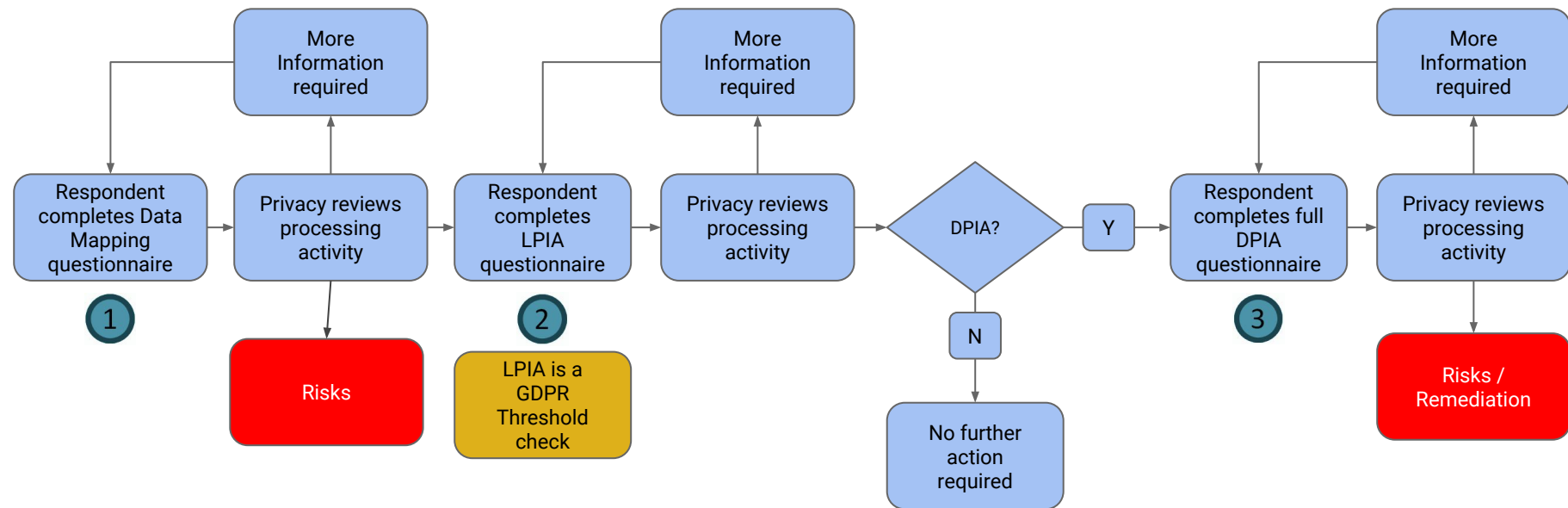
A data subject may object at any time to processing based on the public interest or the controller's legitimate interests, based on grounds related to the individual's particular situation. The controller then has the burden to demonstrate that it has compelling legitimate interests for processing the data that override the individual's interests, rights and freedoms.

First steps and how to become compliant



- ☐ Organization changes for new roles
- ☐ Update contracts with Data processors
- ☐ Do a readiness Assessment
- ☐ Start Data Privacy by Design and Default
- ☐ Data Mapping & Inventory per business function
- ☐ Start compliance for International data transfers
- ☐ **Start Data Privacy Impact Assessments**
- ☐ **Cookie Compliance**
- ☐ Make sure to support 72Hrs breach notifications
- ☐ Secure a DPO if needed

Data processes Assessment : Overall process



Creation

In Progress

Under Review

Risk Tracking

Risk Mitigation

Completed

Cookies management : Current State vs Future State



Name	Type	duration
SESSIONID	Session pointer	Session
WC_ACTIVEPOINTER	Activity pointer	Session

- **Static**
- **Lack of ownership/fragmentation**
- **No way to easily discover new cookies**
- **Lack of transparency to Consumer**
- **Could pose privacy/GDPR risk**
- **Opt-in/Opt-out toggles absent**

Old

Cookies Strictly Needs Session Cookies Analytical Cookies Functional Cookies

COOKIES STRICTLY NEEDS

Technical cookies are strictly necessary for the transmission of communications on an electronic society service provider that, on the explicit request of the contractor or user, provides such service.

Name	Host	duration
OptanonConsent	kitchenaid.it	365 days
OptanonAlertBoxClosed	kitchenaid.it	365 days

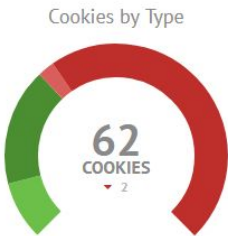
- **Dynamic- ability to push new cookies after audit**
- **Owned by Digital team/Dashboard to InfoSec**
- **Scan discovers new cookies anytime**
- **Full disclosure to consumer**
- **Satisfies GDPR/ePrivacy Directive as understood**
- **Consumer can opt-in/opt-out, strictly necessary**

New

Cookies management: Example from whirlpool.it

Name	Type	Duration	Data Stored	Purpose
SESSIONID	Session pointer	Session	Alpha numeric ID	Track and personalize message to consumer
WC_ACTIVEPOINTER	Activity pointer	Session	Alpha numeric ID	Keep track of actions during the session
WC_AUTHENTICATION_11310563	Authentication	Session	Alpha numeric ID	Authentication ID
WC_PERSISTENT	Persistent info	1 Month	List of Alphanumeric IDs	Persistent id that point to DB for shopping cart items
WC_SESSION_ESTABLISHED	Session Status	Session	True or false	Session active
WC_USERACTIVITY_11310563	Activities list	Session	List of Alphanumeric IDs	User dynamic preferences
__atuvc	Social Share Tag	2 years	Social share tag	AddThis social share
_ga	Analytics	2 Years	Alpha numeric ID	Used to distinguish users
gat* or gat	Analytics	1 Day	Daily analytics	Throttle analytic data request between browser and repos
reevoo_sp_id..*	Product Review	2 Years	Product consumer rating actions	Detail information about functional usage over time
reevoo_sp_ses.*	Product Review	1 Day	Product consumer rating viewed	Session functional information on usage of Reevo
reevoomark_marker	Product Review	1 Month	Product consumer rating marker	Pointer on product which mark for collaboration
wp_cookie_lem	LEM information	3 Months	Informed of WP Cookie usage	Information and awareness of Whirlpool cookie policies
wp_cookie_policy	Cookie Policies	3 Months	Cookie policy read and approve	Acceptance of Whirlpool cookies policies

14 Cookies based on GIS managements with past process



● First Party Session
 ● First Party Persistent
 ● Third Party Session
 ● Third Party Persistent

Cookies Summary

Purpose	Count
Strictly Necessary	1
Performance	5
Functionality	4
Targeting/Advertising	40
Unknown	12
Type	Count
First Party Session	7
First Party Persistent	14
Third Party Session	2
Third Party Persistent	39

62 Cookies based proper scan of 98 pages of the whirlpool.it site



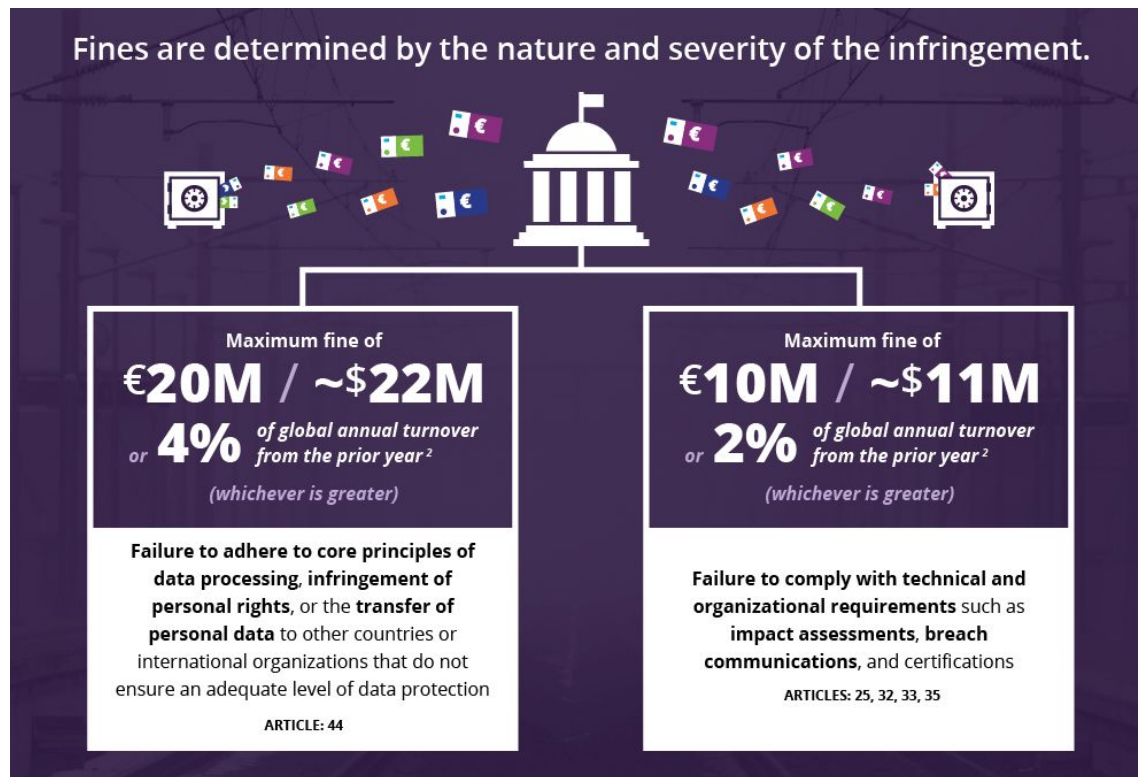
Remedies, liability and penalties

You can no longer say, “it’s not my fault.”



Data subjects can place complaints to Supervisory Authorities

- Right to lodge a complaint with SA (Article 77)
- Right to an effective judicial remedy against a SA (Article 78)
- Right to effective judicial remedy against controller or processor (Article 79)



Embrace 4th Industrial Revolution



- ❑ Become Data privacy compliance trusted for your consumers
- ❑ Have stronger organisation around data usage
- ❑ Continue to innovate with new technology
- ❑ become closer to your consumers