GDPR Training for ITAA

ISME Skillnet and ITAA have collaborated to offer this GDPR Training

- The ISME Skillnet is funded by member companies and the Training Networks Programme, an initiative funded from National Training Fund.
- To avail of the funding and the discounted fee for the training, you are required to complete the participant Profile Sheet and an Evaluation Sheet at the end of the Seminar/Webinar.
- It is important to be aware that you may be called by an independent QA organisation to verify that you have attended the course and to check the quality of the course.

The ISME Skillnet is funded by member companies and the Training Networks Programme, an initiative of Skillnets funded from the National Training Fund through the Department of Education and Skills.

BARBICAN
Data Protection Services

FPLOGUE SOLICITORS

Trainer: Niall Rooney

GDPR & Data Protection Consultant

+353 87 387 1480

www.linkedin.com/in/niallrooney/

Note: These slides and the accompanying presentation contain a general summary and are not legal advice.

Dublin, 27/11/2017

Privacy

> "*the right to be let alone -- the most comprehensive of rights, and the right most valued by civilized men*"

- Olmstead v. US, 1928

> "*the right of the individual to be protected against intrusion into his personal life or affairs, or those of his family, by direct physical means or by publication of information*"

- Calcutt Report, 1990

> Ireland:

- Constitutional right
- Universal Declaration of Human Rights
- European Convention of Human Rights
- Common law or equitable right

Data Protection

The Right to Data Protection

> The protection of individuals in relation to the processing of their personal information is a **fundamental right** in the EU

> But it's not an absolute right

Data Protection Law

> A framework to **balance**

- people's rights
- the needs of society, and
- the legitimate needs of businesses and organisations to process people's personal information

Charter of Fundamental Rights of the European Union

Article 8

Protection of personal data

1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

Article 52

Scope and interpretation of rights and principles

1. Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

The Current Law

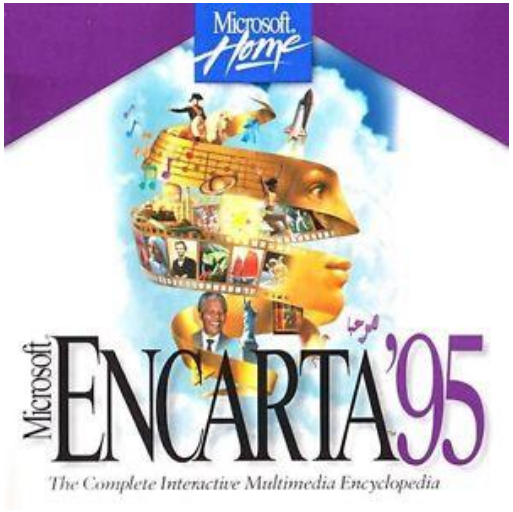
> *Data Protection Directive (95/46/EC)*

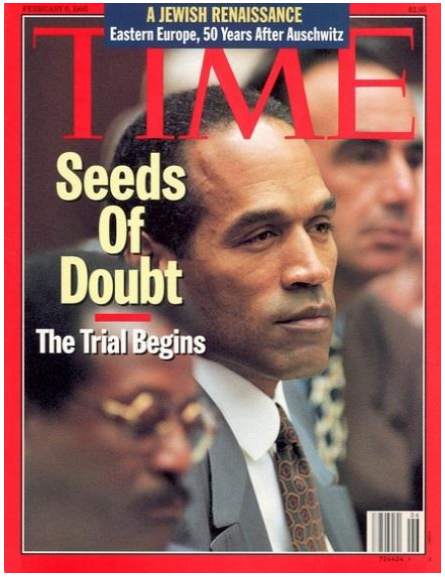
> **Data Protection Acts 1988 and 2003**

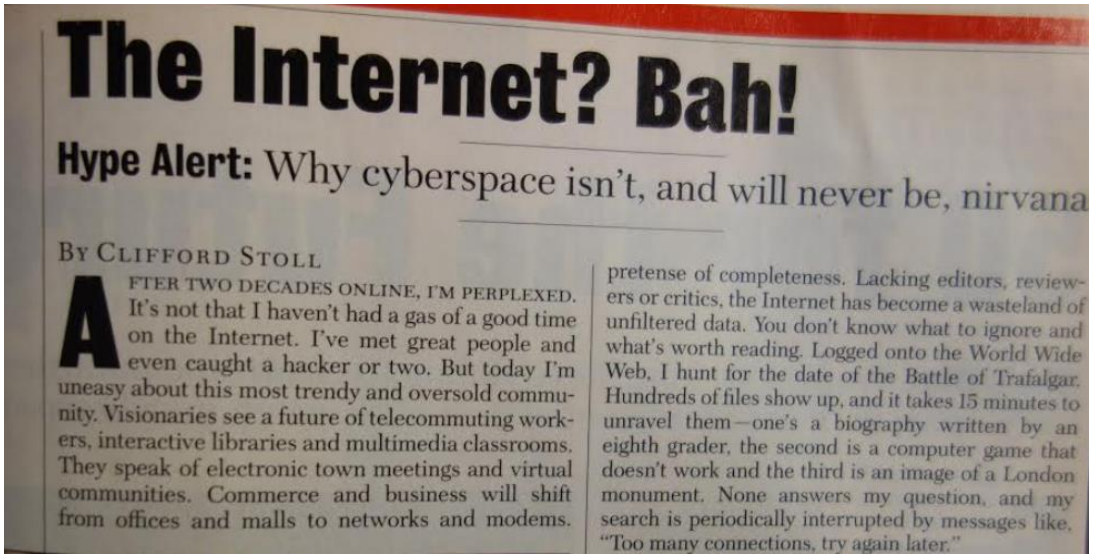
- Data processing principles
- Additional conditions for ‘sensitive data’
- Individuals’ rights including to request a copy of their personal data
- Data Protection Commissioner monitors and enforces compliance
- Data protection policies
- Privacy notices

⇒ ***Why is reform needed…?***

1995…







The Internet? Bah!

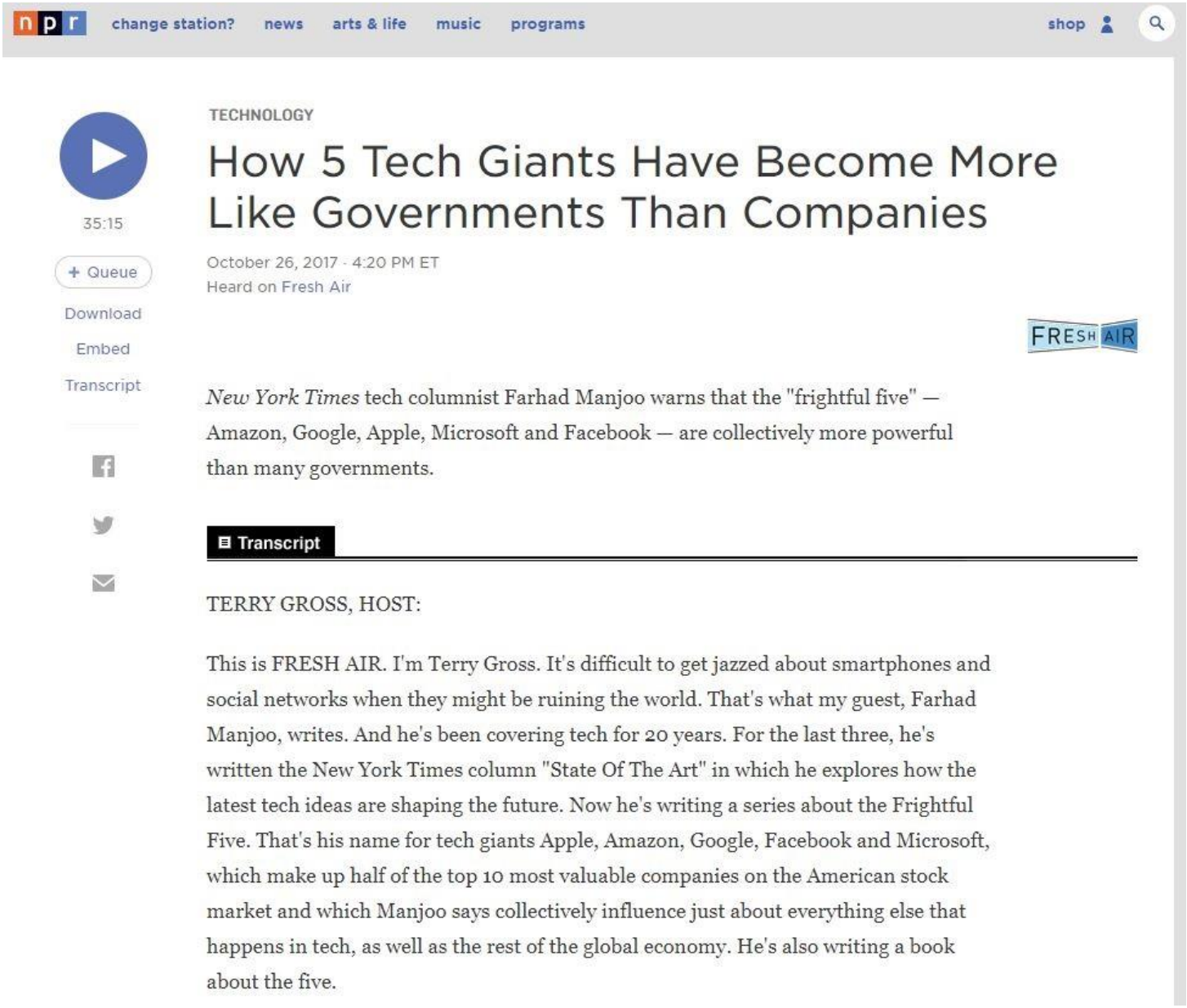
Hype Alert: Why cyberspace isn't, and will never be, nirvana

BY CLIFFORD STOLL

AFTER TWO DECADES ONLINE, I'M PERPLEXED. It's not that I haven't had a gas of a good time on the Internet. I've met great people and even caught a hacker or two. But today I'm uneasy about this most trendy and oversold community. Visionaries see a future of telecommuting workers, interactive libraries and multimedia classrooms. They speak of electronic town meetings and virtual communities. Commerce and business will shift from offices and malls to networks and modems.

pretense of completeness. Lacking editors, reviewers or critics, the Internet has become a wasteland of unfiltered data. You don't know what to ignore and what's worth reading. Logged onto the World Wide Web, I hunt for the date of the Battle of Trafalgar. Hundreds of files show up, and it takes 15 minutes to unravel them—one's a biography written by an eighth grader, the second is a computer game that doesn't work and the third is an image of a London monument. None answers my question, and my search is periodically interrupted by messages like, "Too many connections, try again later."

2017 This Is What Happens In An Internet Minute



http://www.npr.org/2017/10/26/560136311/how-5-tech-giants-have-become-more-like-governments-than-companies

The EU response

> **Rapid technological developments** and **globalisation** have brought new challenges for the protection of personal data.

> Technology allows making use of personal data on **unprecedented scale**.

> People increasingly make their information available publicly and globally.

> This requires a **strong** and more **coherent** data protection framework.

> Backed by **strong enforcement**.

> Creating **trust** to allow the digital economy to develop.

> **People should have control of their own personal data.**

> Enhance legal and practical certainty for everyone.

General Data Protection Regulation (GDPR)

> Regulation (EU) 2016/679

> GDPR applies to the **processing** of **personal data** by **data controllers** and **data processors**

> Will apply in all Member States from **25 May 2018**.

> Builds on existing rules and principles, with significant changes

- increased **compliance obligations** for businesses and organisations
- new and enhanced **rights for individuals**
- increased **regulatory powers** and sanctions

> Directly effective, but…

- Member States may introduce domestic provisions in a number of areas
- **Data Protection Bill 2017**

Who Does the GDPR apply to?

> **Data Controller**

- A person, business or organisation which, alone or jointly, determines the purposes and means of the processing of personal data.
  - Decides and exercises overall control over the ‘why’ and ‘how‘ of a data processing activity.

> **Data Processor**

- A person, business or organisation which processes personal data on behalf of a data controller.

> **Where?**

- Established in the EU, regardless of where processing takes place
- Established outside the EU, if offering goods or services to EU residents or monitoring their behaviour in the EU

What Does the GDPR apply to?

> ***processing***

- includes almost anything you can do with **personal data**, whether or not by automated means
  - collecting, recording, organising, storing, adapting, altering, retrieving, consulting, using, disclosing, erasing, destroying

> ***personal data***

- means any information relating to an identified or identifiable living person ('data subject')
  - **identifiable** means the person can be identified, **directly or indirectly**, including by reference to an identifier, a name, an identification number, location data, an online identifier, or factors specific to a person's identity.

> **special categories of personal data** ('sensitive data')

- data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership
- genetic data; biometric data
- data concerning health
- data concerning a person's sex life or sexual orientation

Some examples of 'personal data'

> Name, address, email, telephone
> Age, gender, marital status
> ID or registration numbers
> PPSN
> Passport number
> Car registration
> Photograph
> Video/CCTV
> Fingerprints, facial recognition
> Travel card or ticket
> Family and lifestyle details
> Education and training information
> Health information, medical reports
> Employment details
> Financial details, bank statements, bank card numbers
> Grades, certificates, testimonials, references
> Online identifiers, IP addresses, cookie identifiers
> RFID tags

Recap: The GDPR applies to –

> the **processing**

- anything you can do with people's personal information

> of **personal data**

- any information about or relating to an identifiable living person who can be directly or indirectly identified

> by a **data controller**

- decides why and how to process personal data

> and a **data processor**

- outsourced processor doing it on behalf and on instructions

Data Controller – Obligations under the GDPR

1) Have a **lawful basis** for processing personal data
2) Comply with **six principles** relating to processing of personal data
3) Be able to show **compliance** with all the principles (‘**accountability**’)
4) Data Protection **by Design** and by Default
5) Data Protection **Impact Assessment** (before high-risk processing)
6) Appoint a **Data Protection Officer**, where required
7) Mandatory data **breach notification**
8) Restrictions on transfers of personal data **outside the EEA**
9) Contracts with **data processors**

(1) Must have a Lawful Basis for processing

> **CONSENT** – the individual has given consent to the processing of their personal data for one or more specific purposes.

> **CONTRACTUAL** – processing is necessary for the performance of a contract to which the individual is party or in order to take steps at the request of the individual prior to entering into a contract.

> **LEGAL OBLIGATION** - processing is necessary for compliance with a legal obligation to which the controller is subject.

> **VITAL INTERESTS** - processing is necessary to protect a person's vital interests.

> **PUBLIC TASK** - processing is necessary for the performance of a task carried out in the public interest or in exercise of the official authority vested in the controller.

> **LEGITIMATE INTERESTS** - processing is necessary for the purposes of the legitimate interests of the controller or a third party, unless overridden by the individual's interests or fundamental rights.

If it's 'sensitive data' also need

> **EXPLICIT CONSENT** – the individual has given **explicit** consent to the processing of their personal data for one or more specific purposes.

> **EMPLOYMENT LAW** – processing is necessary for the carrying out of the obligations and exercising rights of the controller or the data subject in the field of employment, social security or social protection law.

> **LEGAL CLAIMS** – processing is necessary for the establishment, exercise or defence of legal claims.

Consent as a lawful basis

> Consent to processing of personal data
  - must be **freely given, specific**, informed and **unambiguous**;
  - by a statement or a **clear affirmative action**;
  - cannot be inferred by silence, pre-ticked boxes or inactivity
  - **can be withdrawn** and must be **easy to do so**

> Processing of 'sensitive data' requires "**explicit** consent"

> In a written declaration concerning other matters (e.g. a contract), the request for consent must be clearly **distinguishable** from other matters.

> **Records** must be kept of how and when consent was given.

> '*Information society services*' offered directly to a **child** < 16 years*, must get verified consent of parent or guardian.

* Member States may provide for a lower age, provided not < 13 years

(2) Must comply with the Six Principles

a) LAWFULNESS, FAIRNESS & TRANSPARENCY

- Personal data must be processed lawfully, fairly and in a transparent manner.

b) PURPOSE LIMITATION

- Personal data must only be collected for specified, explicit and legitimate purposes, and not further processed in any way incompatible with them.

c) DATA MINIMISATION

- Personal data must be adequate, relevant and limited to what is necessary for the purposes for which it is processed.

d) ACCURACY

- Personal data must be accurate and, where necessary, kept up to date, with inaccurate data erased or corrected without delay.

e) STORAGE LIMITATION

- Personal data must be kept for no longer than is necessary for the purposes for which the data is processed.

f) SECURITY, INTEGRITY & CONFIDENTIALITY

- Personal data must be processed in a way that ensures appropriate security.

(3) Accountability – Data Controller

> Be able to demonstrate compliance with all six data processing **principles**

> Implement appropriate **technical and organisational measures** to ensure:
  - that processing complies with the GDPR's requirements; and
  - a level of security appropriate to the risk

> Internal **policies** and processes

> Maintain **documentation** and records of compliance

> Specific **records** of processing activities (where **Art 30** applies)

> Staff **training** and awareness

> Testing and **auditing**

> Data protection **by design** and by default

> Data Protection **Impact Assessments**, where appropriate

> **Data Protection Officer**, where required

Records of Processing Activities (Article 30)

> Data controller must maintain a **record** of all processing operations

> Make the record **available** to the supervisory authority on request

> **Specific information** required, including

- Name and contact details, including DPO if relevant
- The purposes of the processing
- Recipients or categories of recipients of the personal data
- Details of non-EEA data transfers and safeguards in place
- Where possible, time limits for erasure of data
- Description of the technical and organisational security mechanisms in place

> Exempt if employ < **250** persons, **unless** the processing carried out

- is likely to result in a risk to the rights of data subjects;
- is not occasional;
- includes sensitive data or data relating to criminal convictions

Recap: Processing of personal data must –

(A) Have a LAWFUL BASIS *	(B) Comply with the six PRINCIPLES
The individual has given **consent ***	1) **Lawfulness, fairness & transparency**
Necessary for the performance of a **contract** with the individual or to enter into such a contract	2) **Purpose limitation**
Necessary for compliance with a **legal obligation** to which the controller is subject	3) **Data minimisation**
Necessary to protect a person's **vital interests**	4) **Accuracy**
Necessary for performance of a task in the **public interest** or in exercise of **official authority** vested in the controller	5) **Storage limitation**
Necessary for purposes of **legitimate interests** of the controller or a third party, except where overridden by the interests of the individual **	6) **Security, integrity & confidentiality**

* Explicit consent required if it's 'sensitive data' (e.g. health)

& **(C)** Controller must be able to **demonstrate compliance** with the principles ('**ACCOUNTABILITY**')

'Direct Marketing'

> *Any advertising or marketing communication (whether trying to sell or promote) directed to particular individuals or businesses.*

> **A separate law**: Electronic Privacy Regulations 2011 (S.I. 336 of 2011)

> Unsolicited emails or texts for purpose of direct marketing:

- → Individual **OPT-IN**
- → Individual (business email address, commercial relevance) **OPT-OUT**
- → Individual, existing customer (12M), similar product, gave Opt-Out when collected details, and Opt-Out in every message '**SOFT OPT-IN**'
- → Business ('not a natural person') **OPT-OUT**

> *Will be updated by a new ePrivacy Regulation (EU) in 2018*

> **And -- the GDPR <u>also</u> applies !**

(4) ‘Data Protection by Design and by Default’

> The GDPR aims to establish a culture of privacy by design and default.

> Embed data privacy into operational processes from the very start.

> Data protection and privacy in mind at every step of the planning and operation of data processing activities.

> '***Privacy by design***' requires controllers to implement appropriate technical and organisational measures which are designed to implement the data protection principles in an effective manner.

> '***Privacy by default***' requires controllers to implement appropriate technical and organisational measures to ensure that, by default, only personal data which is necessary for each specific purpose of the processing is processed.

(5) Data Protection Impact Assessments

> Where processing operations likely to result in a **high risk** to the rights of individuals, data controller must, **prior to processing**, carry out a DPIA

> Specifically required when controller engages in:

- Automated processing, including profiling, that produces legal or other significant effects for a data subject;
- Large scale processing of sensitive data or data relating to criminal convictions;
- Large scale, systematic monitoring of a publicly accessible area.

> Where DPIA indicates a high risk is likely, controller must consult with the supervisory authority (DPC) prior to processing.

(6) Data Protection Officer (DPO)

> DPO appointment is **mandatory** for
  - Public bodies (except courts), and
  - Businesses and organisations that, as a **core activity**, monitor individuals **systematically** and on a **large scale**, or that process **sensitive data** on a **large scale**.

> Appointment, position and tasks of DPO are set out in the GDPR.
  - 'expert knowledge of data protection law and practice'
  - be involved in all data protection issues
  - report directly to highest level of management
  - operational independence, no conflicts of interest, confidentiality
  - inform and advise; monitor compliance; point of contact for individuals/DPC

> May appoint DPO on a voluntary basis, but the GDPR requirements still apply as if mandatory.

(7) Data Breach Notification

> **Personal data breach**
  - a 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

> Data controller must **notify** a personal data breach to the supervisory authority (DPC) within **72 hours** of becoming aware of it.

> If notified later, must give reasons for the delay.

> Notification requires certain minimum information.

> In “high-risk” cases may have to inform affected individuals.

> Notification is **not** required where the personal data breach is unlikely to result in a risk to the rights of individuals.

> Data controller must **document** any personal data breach, including the facts, its effects and remedial action taken.

61% of organisations had data breach in 2016 - survey

Updated / Thursday, 19 Jan 2017 **20:48**

61% of organisations have had at least one data breach

Almost two thirds (61%) of organisations have had at least one data breach in the last year, an increase on the previous year, according to a new survey of 200 professionals.

The survey was carried out by the Irish Computer Society (ICS), which also found that more than half of the breaches were caused by staff members misplacing records.

(8) International Data Transfers

> GDPR imposes restrictions on transfers of personal data **outside the EEA** to ensure that the level of protection of individuals is not undermined.

> Transfers may be made where Commission decides that a country ensures an **adequate level of protection**.

> Otherwise, transfers permitted where the organisation receiving the personal data has provided 'appropriate safeguards'

- Individuals' rights must be enforceable and effective legal remedies for individuals must be available following the transfer.
- Appropriate safeguards may be provided for by binding corporate rules (BCRs; model clauses approved by the Commission; compliance with approved codes of conduct and certification schemes

> Derogations for specific situations

- explicit consent to transfer
- contractual necessity
- public interest reasons
- legal claims defence
- vital interests

(9) Contracting with Data Processors

> Whenever use a processor, must have written **contract** setting out:

- the subject-matter and duration of the processing
- the nature and purpose of the processing
- the type of personal data and categories of data subjects
- the obligations and rights of the data controller.

> GDPR sets out **mandatory terms** for contract requiring processor to:

- process data only on documented instructions from controller;
- ensure processor's staff are committed to confidentiality;
- take all appropriate security and organisational measures;
- sub-contract only with prior permission of controller;
- assist controller in complying with data subject rights;
- assist controller in complying with its data breach notification obligations;
- delete or return all personal data to controller, if requested, at the end of the processing;
- make available all information necessary to demonstrate compliance with processing obligations and allow audits to be conducted by controller

Data Processor - Obligations under the GDPR

> Must implement appropriate technical and organisational measures ensuring
  - processing complies with the GDPR
  - protection of the rights of individuals
  - a level of security appropriate to the risk

> Mandatory records of processing activities for some (Article 30)

> Only process in accordance with documented instructions of controller

> Processing must be based on a contract

> GDPR provides a list of mandatory terms that must be included

> Not engage sub-processor without prior written authorisation

> Notify data controller without undue delay of a personal data breach

> Appoint a Data Protection Officer, where required

> Restrictions on transfers of personal data outside the EEA

Individuals' Rights under the GDPR

1) **Information** (***Privacy Policy***)
2) **Access their own personal da**ta (***Subject Access Request***)
3) Correct their personal data
4) Erase their personal data ('right to be forgotten') *
5) Restrict data processing *
6) Object to data processing *
7) Export their personal data to another data controller (data portability) *
8) Not be subject to automated decision-making, including profiling *
9) Be notified of a data security breach *
10) **Make a complaint** to the supervisory authority (DPC)
11) **Sue controller or processor for damages** resulting from breach of GDPR

Privacy Policy / Statement / Notice (Information)

- Data controller identity and contact details.
- DPO contact details, where applicable.
- Purpose of processing.
- Lawful basis for processing.
- Legitimate interests, where applicable.
- Recipients or categories of recipients.
- Details of transfers out of the EEA, safeguards in place and he means by which to obtain a copy.
- Data retention period, or criteria used to determine it.
- Individual's rights including access, correction, erasure, restriction, objection, data portability.
- Where processing based on consent, right to withdraw it at any time.
- Right to complain to the DPC.
- Whether data controller uses automated decision-making (including profiling), information about the logic involved, and the consequences for the individual.
- Whether the provision of personal data is a statutory or contractual requirement or obligation, and the consequences of failure to provide such data

- Fair and transparent processing principle
- GDPR increases the amount of information that must be provided
- Must provide in an easily accessible form, using clear and plain language

Subject Access Requests

> Individuals have the right to obtain from a data controller
  - confirmation that their personal data is being processed;
  - **a copy of their personal data**; and
  - other specified **information**, including purpose(s); recipients(s); retention period; individuals' rights; where data transferred out of EEA, the appropriate safeguards

> Motive for the request is irrelevant

> **No fee**

> Data controller must respond within **one month**

> May extend by two months where requests are complex or numerous

> Where request "manifestly unfounded or excessive" can
  - charge a reasonable fee taking into account administrative costs, or
  - refuse to respond

> If refuse to respond, must explain why and inform individual of their rights

Erasure (right to be forgotten)

Data controller must erase personal data on request where:

> The data is no longer necessary for the purposes it was collected for.

> The data subject withdraws consent and there is no other lawful basis for the processing.

> The data subject objects to the processing and there are no overriding legitimate grounds for the processing.

> The data subject objects to the processing for direct marketing purposes.

> The personal data has been unlawfully processed.

> The personal data must be erased for compliance with a legal obligation under EU or relevant national law.

> The personal data has been collected in relation to the offer of information society services directly to a child.

Unless continued retention is necessary for

> Exercising the right of freedom of expression and information.

> Complying with a legal obligation under EU or member state law.

> The performance of a task carried out in the public interest.

> Exercising official authority vested in the data controller.

> The establishment, exercise, or defence of legal claims.

> For public health reasons.

> For archiving purposes in public interest, or scientific/historical research, or statistical purposes

Right to lodge a complaint with the DPC

> Individuals have right to lodge a complaint with the supervisory authority if they consider their personal data has been processed in a way that does not comply with the GDPR.

> Supervisory authority must inform the complainant on the progress and the outcome of the complaint.

> Individual has the right to take legal action against a legally binding decision of the supervisory authority concerning him or her

> Individual has the right to take legal action where the supervisory authority fails to deal with a complaint or fails to inform the individual within 3 months of the progress or outcome of the complaint.

Right to Sue the Data Controller / Data Processor

> Individual may **sue** for infringement of rights under the GDPR resulting from processing of their personal data in non-compliance with the GDPR

> Right to receive **compensation** from controller or processor for damage suffered (material and non-material) as a result of the breach of the GDPR

> A controller or processor will be exempt from liability if can prove not “in any way” responsible for the event giving rise to the damage

> Processor only liable insofar as has failed to comply with its specific GDPR obligations or has acted outside of its instructions

> Where both a controller and processor engaged in same processing, and both responsible for the damage, they will be jointly liable for entire damage.

> Potential for group legal actions is also facilitated by the GDPR

Powers of the Data Protection Commissioner

Investigative powers

> Conduct investigations and audits

> Obtain access to data, premises and processing equipment

Corrective powers

> Issue warnings and reprimands

> Order compliance with individual's requests

> Order communication of a data breach to an individual

> Impose a temporary or permanent ban on processing

> Order rectification or erasure of personal data

> Suspend data transfers to a third country

Administrative fines

> May impose fines ('*effective, proportionate and dissuasive*') on data controllers and data processors for non-compliance

> Up to €10m/€20m or 2%/4% of total worldwide annual turnover

Helen Dixon - Data Protection Commissioner for Ireland
Irish Independent, 27 April 2017

Are you willing to go the full distance in fining companies €20m?

Yes. We have to be willing to… it's absolutely the case that we will be imposing fines against **big and small** entities based on the issues that come across our desk and the areas of risk we identify. **There's nothing surer than this**.

Will there by any leeway to ease companies into the new, stricter punishment regime?

No. There's not going to be any amnesty or first or second chances. On the other hand, the GDPR does set out **criteria** when we go to look at the **quantum** of fine we might impose. We are **obliged to take into account** the level of co-operation between us and the regulated entity, the number of data subjects, the level of effect on the data subjects and any previous contraventions.

Key GDPR Takeaways for Business

> Requires a shift in **mindset** about people's data privacy

> It's **principles-based** and **risk-based**

> Collecting, using and keeping personal data now has a **cost**

> **Individuals** have more **control** with stronger **rights**

> Increased **regulatory sanctions** and powers.

> Processing needs a **lawful basis** and must comply with **six principles**

> Data controllers must be able to demonstrate their **accountability**

> More difficult to rely on **consent** as a lawful basis

> **Privacy Policy / Notice** needs much more information

> **Security** measures and data breach plan

> **Data processor** contracts and mandatory terms.

> Mandatory **Data Protection O**fficer for some.

Preparing for the GDPR

1) **Understand Your Current Data Processing Activities**
2) **Assess Your Current Compliance with GDPR**
3) **Prioritise the Remedial Actions**
4) **Implement an Action Plan to Move Towards Compliance**

More Information

> **Data Protection Commissioner** (Ireland)
- www.dataprotection.ie
- www.gdprandyou.ie

> **Information Commissioner's Office** (UK)
- www.ico.org.uk (click on '→ Getting Ready for the GDPR')
- https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf

> **Full Text of the GDPR**
- http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN