



GDPR - A Guide to Compliance

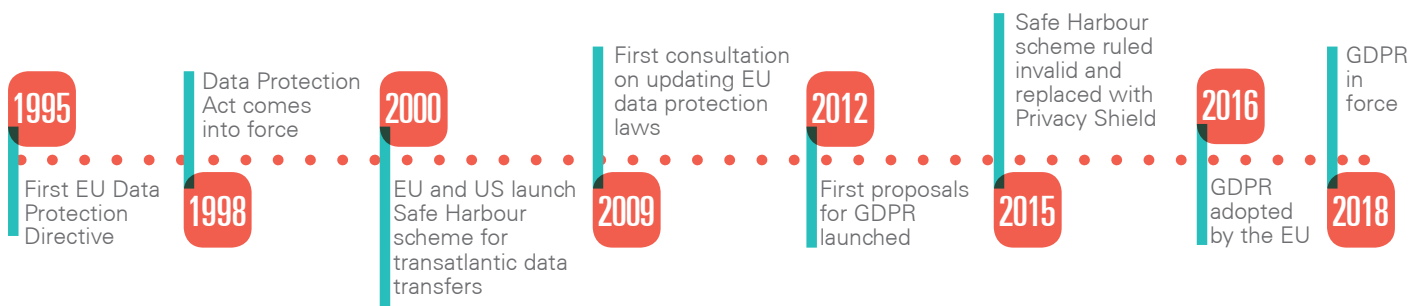
Understanding data protection law in the EU

What's inside?

Introduction	2
Summary of GDPR	3
Conditions for processing data	5
General data protection principles	6
Consent	7
Marketing	8
New rights	8
Privacy	9
Rules for data processors and controllers	9
Data protection officers	10
International data transfers	11
Supervisory authorities	12
Managing risk	13
Breaches and sanctions	14
GDPR compliance checklist	15

Introduction

The General Data Protection Regulation (GDPR) proved a major shakeup in data protection laws across all Member States of the EU. It officially came into force on 25 May 2018, and as a Regulation, automatically applied in every Member State. Furthermore, a business based outside the EU may be required to appoint a representative, generally referred to as a Data Protection Officer (DPO), based in the EU who is accountable for data protection.

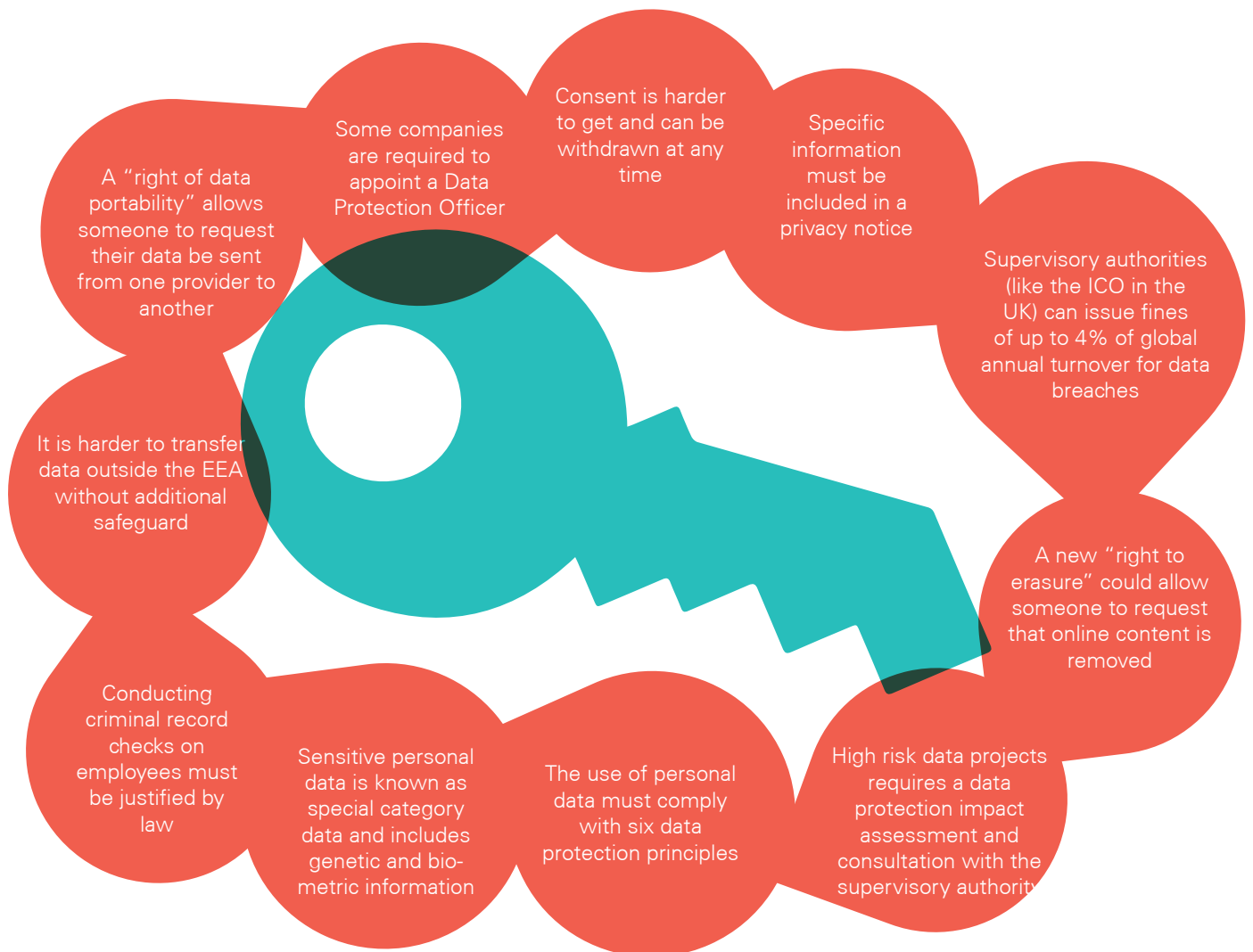


In the UK, GDPR was implemented into law as the Data Protection Act 2018. Designed to be read alongside each other, the DPA 2018 and GDPR provide the foundation for data protection law in the UK, along with the powers of the Information Commissioner's Office to set guidance and root out wrongdoing.



GDPR's reach is global. Any company that offers goods or services to anyone in the EU will be required to comply.

Summary of GDPR



About people's rights

GDPR represents a fundamental shift in how the use of personal data is regulated. The people who give data, data subjects, own their data and are simply lending it to others for use. Carrying out activities with people's data that could cause them harm, not securely stored, used in a way they would not expect or were not told about, or packaged up and sold for profit, is expressly forbidden by GDPR.

Offering goods and services in the EU

Under Article 3(2) of GDPR, GDPR applies to:

“the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union;

the monitoring of their behaviour as far as their behaviour takes place within the Union”

Appointing a representative

If a company is based outside the EU and is covered by GDPR, then a representative of that company must be appointed in the EU. The representative will be required to deal with the supervisory authority and accept liability for breaches.

How do I know if my business offers goods or services to the EU?



Language

Using an EU language which is not relevant to customers in your home state (e.g. a US-based website in Slovakian).



Domain name

The website has a top level domain name of an EU member state (e.g. using .nl or .fr).



Currency

Displaying prices in Euros or another EU currency.



Delivery in the EU

Delivery of physical goods to an EU address.



Reference to citizens

Mentioning customers including customer testimonials from EU citizens.



Customer base

A large proportion of customers are EU citizens.



Targeted advertising

Adverts are directed at EU citizens (e.g. adverts in a local newspaper).

Conditions for processing data

Use of any personal data must be justified using one of the following conditions for processing:

-  **1** The person gave **consent**
-  **2** To fulfil or prepare a **contract**
-  **3** There is a **legal obligation**
(excluding a contract)
-  **4** To save someone's life or in a **medical situation**
-  **5** To carry out a **public function**
-  **6** There is some other **legitimate interest**
(excluding public authorities)

If the data is "special category data", i.e. about a person's race, religion, or health status, there must be an additional justification to process the data which can include explicit consent, employment law, or for medical purposes.

- What to do:**
- ✓ Document which conditions you can rely on for using data
 - ✓ Ensure that you have additional justification for special category data

Where should these conditions be documented?

It is very important to identify which condition for processing is being relied on. This is the kind of information that is expected to be included in a privacy notice. If relying on consent, the person must be told they can withdraw their consent at any time.

What counts as legitimate interest?

To rely on this condition, you must properly balance the interest of the data controller with the right to privacy for the individual. One way to test if something may count as a legitimate interest is to consider whether the individual would reasonably expect and allow their data to be used in that way.

General data protection principles

In addition to being justified through the **conditions for processing**, using personal data must follow all of the six general principles.

1

Lawful, fair, and transparent

Data collection must be fair, for a legal purpose and be open and transparent about how the data will be used

2

Limited for its purpose

It can only be collected for a specific purpose

3

Data minimisation

Data collected must be necessary and not excessive for its purpose

4

Accurate

It must be accurate and kept up to date

5

Retention

Data should not be stored any longer than necessary

6

Integrity and confidentiality

Data must be kept safe and secure

It is not enough just to comply with all six of these principles; you must be able to show how you comply with them. This means having policies about how personal data is managed and making sure that there is a clear compliance structure, responsibilities are allocated, staff are trained and systems have been audited. It also means bringing in technical measures to improve safety and security, and ensuring individuals can properly access their data. Refresher training should be carried out at least once a year.

What to do:

- ✓ Ensure that up to date technical systems are being used
- ✓ Make sure company policies on personal data will be updated in reference to the six data protection principles

Consent

GDPR strengthens the level of consent that is required to justify using personal data.

Consent must be **freely given** and **specific**. There must be a **genuine choice**, the person cannot be **coerced** or unduly **incentivised** or **penalised** if consent is refused. If consent is taken as a **condition of subscribing** to a service, then the organisation must demonstrate how consent was freely given.

Will old consent still be valid?

Personal data that has been collected before GDPR comes into force will still be valid only if it meets the requirements of the new Regulation. This could be hard to check and it is likely that new consent will have to be secured, or a different condition relied upon.

Consent can be withdrawn at any time without the person suffering any negative consequences as a result. If this is not the case, then consent is not the right condition.

Not consent:

- ❌ A pre-ticked box
- ❌ Silence or inactivity
- ❌ Complex or technical language
- ❌ Tied to a contract
- ❌ Bundled with consent for other purposes
- ❌ Will be detrimental to the individual if they do not give consent or withdraw it

Consent

- ✅ Separate from any other parts of a form or contract
- ✅ Specific consent for each activity to be undertaken with the data
- ✅ Authorised by a parent for someone under 16 years old
- ✅ Explicitly given to process sensitive data as well as personal data

Example:



If you do not wish to receive further marketing information from us, please tick "opt-out".



Tick if you would like to receive information about our products and special offers by post | by email | by telephone | by text | by fax

Consent and criminal record checks

GDPR will make it harder to justify routine criminal background checks. It is not satisfactory to rely on the consent of the individual to process their criminal record, it must instead be authorised by law.



- What to do:**
- ✅ Review the ways you obtain consent and assess whether these will be valid under GDPR. If not, change your procedures.
 - ✅ Make sure there is a procedure in place for acting on a request to withdraw consent

Marketing

Consent and marketing can be complicated. To prove consent has been given, some firms operate a “double opt-in” model. After initial consent is given, an email is sent to the individual asking them to click a link to validate that consent.

It will be more difficult to justify automated targeting or profiling of people using their personal information. The reasons for making automated decisions about a person must be explained. For example, targeting adverts for baby products at someone who searches for ‘morning sickness’ online may be unlawful profiling based on the collection of sensitive personal information.

Often other conditions for processing, such as legitimate interest, can work better for marketing than consent. Marketing similar products or services to customers can be justified under legitimate interest. However email marketing is dying, and many companies are avoiding this entire issue by engaging with their customers directly on social media.

Data subject rights

Data portability

There is a new right called data portability under GDPR. While people already had the right to access their data through a subject access request, now it will have to be provided in a way that makes it easy for a computer to read (e.g. via a spreadsheet). A person can also request for their data to be transferred directly to another system for free. This could mean transferring all of your photos from one social network to another, or content from one cloud provider to another.

Right to erasure

Sometimes referred to as the “right to be forgotten,” this is one of the most talked-about innovations of GDPR. Also known as the right to erasure, it means that someone can request the deletion or removal of their personal data, including information published or processed online.

Google’s GDPR fine

Six minutes after GDPR came into force, Google, along with WhatsApp, Instagram and Facebook, had complaints launched against them alleging they were not giving users a free choice when collecting their data in a practice known as ‘forced consent’ - where a user must either agree or be barred from using the service. In January 2019, the French authorities agreed and fined Google 50 million.



What to do:  Ensure there are procedures for dealing with data subject rights

Privacy

Privacy notices, or “how we use your information” guides must be given at the point of data collection. The condition for processing must be included in the privacy notice, as well as the person’s rights and how they can make a complaint. For instance, if you rely on consent for using their data, you must inform the person of their right to withdraw consent at any time. Organisations must undertake Privacy Impact Assessments when conducting risky or large scale processing of personal data.



Privacy by design

Privacy by design means that each new service or business process that makes use of personal data must take the protection of such data into consideration during the design phase.



Privacy by default

Organisations must ensure that, by default, privacy settings should be set to high. Only personal data that has a purpose should be collected and retained; and only for the minimum time necessary for those purposes. In particular, personal data should not be automatically accessible to anyone on the internet. No manual change to the privacy settings should be required on the part of the user.

- What to do:**
- ✓ Ensure privacy by design and privacy by default procedures are fully implemented
 - ✓ Ensure privacy notices contain all necessary information and are given at the right time

Data processors and controllers

Some industries and positions, such as payroll or accountancy, generally deal with data collected by third parties. These are known as **data processors**, as opposed to **data controllers** who collect personal information and decide what it is used for. Processors only use data collected from another company and were often exempt from data protection rules prior to GDPR coming into force.

GDPR applies directly to data processors. There must be a contract in place between a data controller and processor, including specific clauses relating to data protection, and processors may be liable for compensation claims.

If you have contracts with data processors, check if they are compliant with GDPR. Data processing agreements between controllers and processors can either be a separate agreement, or included in standard contracts.

- What to do:**
- ✓ Ensure there are data processing agreements between controllers and processors

Data Protection Officers

Data Protection Officers are responsible for everything related to keeping data secure in the company. GDPR strengthened the role of Data Protection Officers. They report directly to the highest levels of management and cannot easily be dismissed. DPO's cannot be shareholders, executives or board members. They must act independently. External organisations can also be appointed as DPO.

Data Protection Officer job descriptions

dyson


"The DPO should achieve efficient management of Dyson information, while optimising its effectiveness and maintaining compliance with global information-related laws and regulations."


British Gas

"The DPO will provide pragmatic and commercially-focused privacy and data protection advice across British Gas and Centrica."

A DPO must be appointed when:

- Processing is carried out by a public authority
- Large scale regular and systematic monitoring is the core of the processing activities of the controller
- Sensitive data on a large scale is at the core of the processing activity

What to do:  Consider if a DPO must be appointed and keep this under regular review

International data transfers

Transferring data outside the EEA is subject to strict restrictions under GDPR. Essentially it cannot be done unless there are specific protections put in place.

Data should not be transferred outside the EEA without ensuring it will be adequately protected

You may still be liable for data that is transferred onwards after it has already been sent to a third country

Binding Corporate Rules where companies commit to complying with GDPR can be relied on to justify transferring data outside the EEA

Transferring data to the US

The Privacy Shield replaced the previous US-EU Safe Harbour Scheme which was ruled invalid by the European Court of Justice in 2015. The Privacy Shield covers buying goods or services online, using social media or cloud storage, transferring data, and employees of EU-based companies that use US companies to deal with personal data. US-based organisations can join the Privacy Shield Framework through a self-certification process.

What to do: ✓ Consider how GDPR may impact on any international data transfers you carry out

Supervisory authorities

Under GDPR, each Member State is required to have a designated independent regulator to be the supervisory authority (SA). In the UK this is the Information Commissioner's Office (ICO). If a business operates in multiple Member States, it should have a SA as its "lead authority" based on the main establishment of the business. This "lead authority" acts as a **one-stop shop** to supervise all processing activities in its locations throughout the EU, though another SA may take control if it relates primarily to their jurisdiction.

Who is in charge?

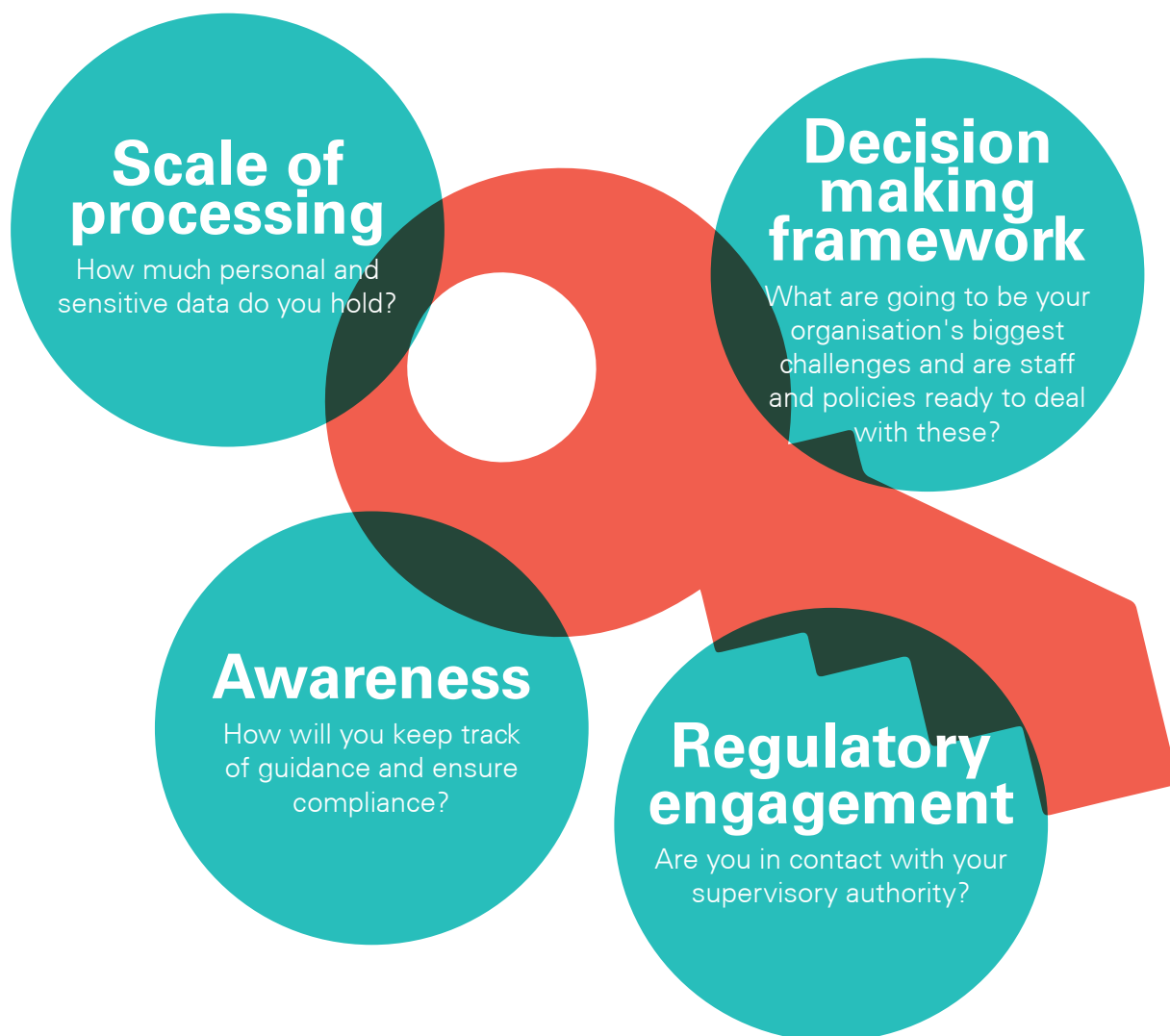
Ireland is home to the European headquarters of many major international corporations including Microsoft, Google, Facebook, PayPal, Apple, Yahoo, and more. Therefore the Irish authorities (Data Protection Commissioner Ireland) might be responsible for any major breaches or investigations. However if there was a data protection issue relating just to Facebook in Spain for instance, then the Spanish SA could oversee it.



What to do: ✓ Understand where your main establishment is and who your lead supervisory authority will be

Managing risk

It is recommended that organisations carry out an audit of all the data they hold around once a year. This should include reviewing how the data is processed and stored. Some key things to consider:



Auditing the information you hold and compiling a [data register](#) including what data you do hold, where it is stored, how it is used and by whom, can be a helpful tool.

- What to do:**
- ✓ Think about how you manage risk and how data protection is dealt with in your risk assessment framework
 - ✓ Consider a data audit and data register

Breaches and sanctions

GDPR has a strict sanctions regime. **Supervisory authorities** such as the ICO can fine a company up to 4% of annual worldwide turnover, or €20m, whichever is greater. Sanctions can also include audits, warnings, and temporary or permanent bans from processing data.

GDPR introduced the requirement for serious or major breaches to be reported. In January 2019 Google received a €50 million fine for GDPR violations.

Reportable

The loss of an unencrypted laptop or digital media with the names, addresses, and dates of birth of over 100 people.

Not reportable

The loss of a marketing list of less than 100 names and addresses where there is no particular sensitivity of the data.


Even if small amounts of sensitive data are at risk, such as health records, there should be a presumption to report. Consider if the release of such data could cause significant risk of individuals suffering substantial detriment or distress.

Breaches are not made public. However if regulatory action is taken, such as a fine or warning, then this could be made public.

How do I demonstrate compliance?

1 Review and, when necessary, update company policies that deal with how personal data is collected, handled and stored.

2 Document a clear compliance structure that includes: allocation of staff responsibility, auditing of current practices, and crucially, training for all relevant staff.

What to do:  Ensure all staff are adequately trained on GDPR for their specific job role and re-train at least once per year.

GDPR compliance checklist



Review the ways you obtain consent and assess if these will be valid under GDPR. If not, change your procedures.



Consider what alternative conditions you can rely on for using personal data.



Check if you collect any genetic or biometric information and implement procedures for protecting sensitive personal data.



Make sure there is a procedure in place for acting on a request to withdraw consent.



Make sure company policies on personal data have been updated to comply with the six data protection principles.



Consider privacy by design and privacy by default in new and existing applications.



Ensure there are procedures for dealing with data portability and right to be forgotten requests.



Consider the role of your Data Protection Officer, whether they have sufficient budget and authority. If you do not have a DPO, consider whether to appoint one.



Review and update your privacy notices.



Review any current or future contracts with data processors.



Think about setting up a central data breach management register.



Understand where your main establishment is and who your lead supervisory authority will be.



Consider how GDPR impacts on any international data transfers you carry out.



Think about a data audit and data register for your organisation.



Consider how you manage risk and how data protection is dealt with in your risk assessment framework.



Ensure staff train on GDPR at least once a year.

Further resources

European Commission Reform of EU Data Protection Rules:

http://ec.europa.eu/justice/data-protection/reform/index_en.htm

ICO Overview of the General Data Protection Regulation:

<https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/>

Website of the EU GDPR:

<http://www.eugdpr.org/>

EU-US Privacy Shield:

<https://www.privacyshield.gov/welcome>

Article 29 Working Party:

http://ec.europa.eu/justice/data-protection/article-29/index_en.htm

GDPR Staff Awareness Training

To help organisations maintain GDPR compliance, VinciWorks regularly updates its GDPR training suite. From an in-depth modular course to short five-minute knowledge checks, our GDPR training suite allows organisations to train their entire staff on GDPR. This includes general staff and staff who require specialised training, such as HR, IT, marketing and more. Further, VinciWorks has added training catered to businesses with US-based staff.

<http://vinciworks.com/GDPR>

VinciWorks is a leading global provider of online compliance training. With over 80,000 users across 70 countries, VinciWorks has established itself as the definitive authority in compliance learning.

By facilitating collaboration between leading firms, VinciWorks creates courses that satisfy regulatory requirements and remain current.

VinciWorks' core suite of compliance courses includes:



Anti-money
laundering



Anti-bribery
and corruption



Equality &
diversity



Information
security



Data
protection



Cyber
security



Modern
slavery

To learn more visit www.vinciworks.com



VinciWorks

Innovative risk and
compliance solutions

www.vinciworks.com

enquiries@vinciworks.com

+44 (0) 208 815 9308