VinciWorks

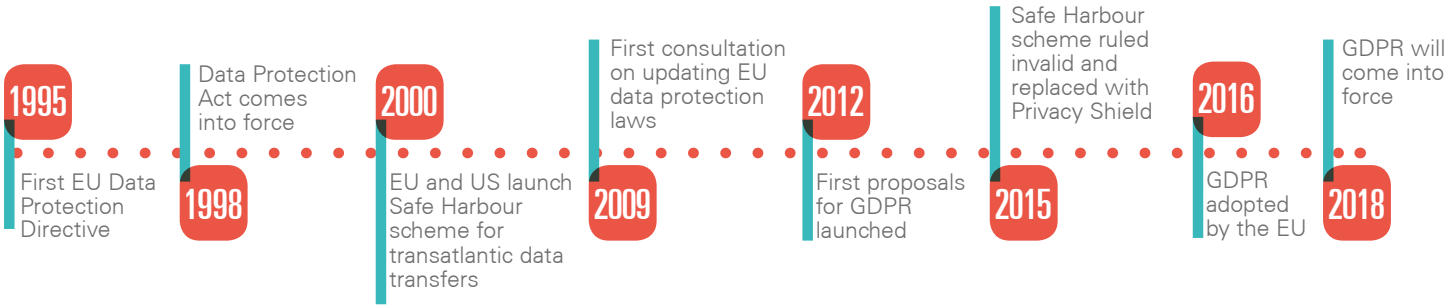
GDPR - A Guide to Compliance

Understanding data protection changes in the EU

What's inside?

Introduction

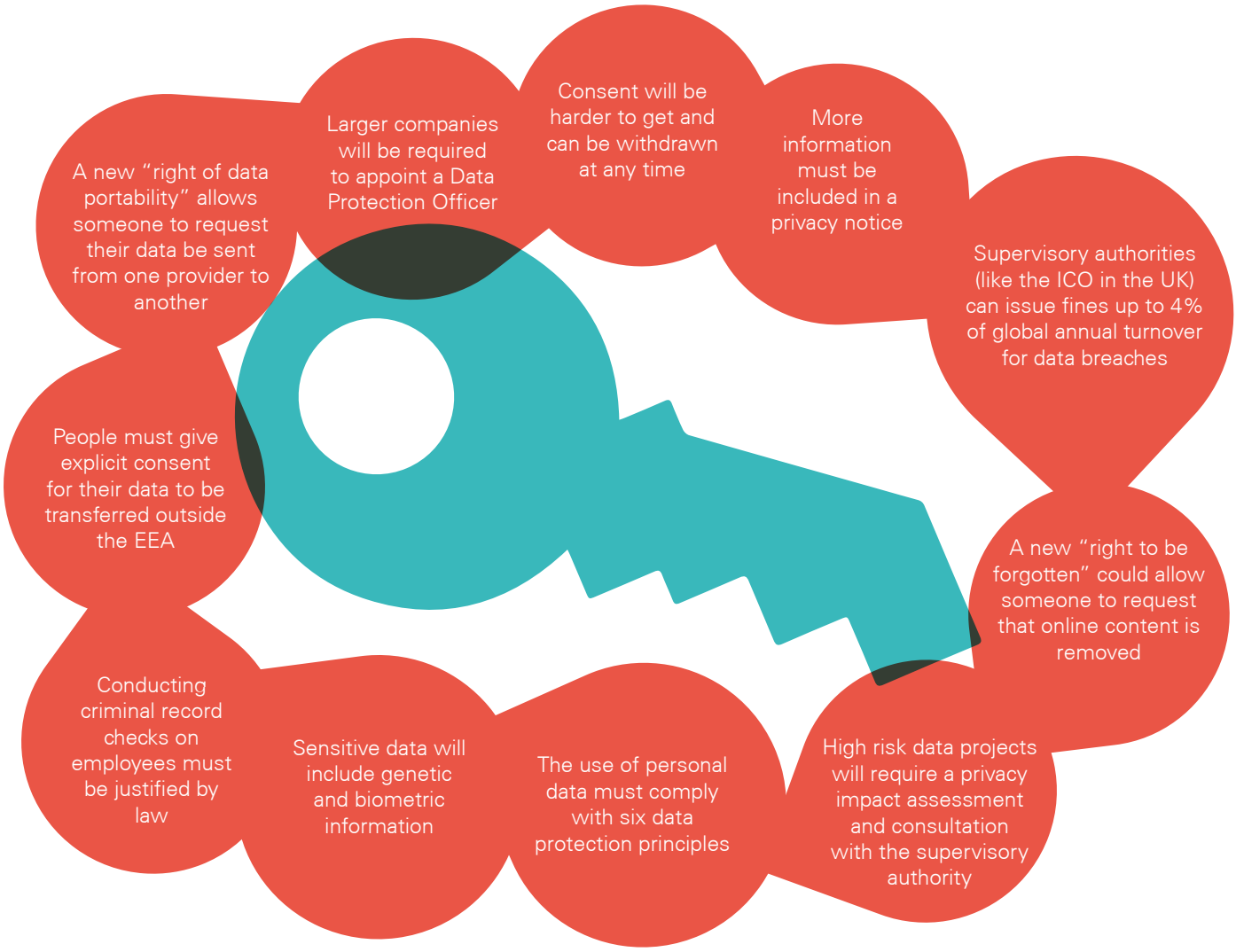
It has been over 20 years since the EU last set standards for data protection in the Data Protection Directive 1995, which in the UK became the Data Protection Act 1998. Since then there has been a revolution in data and how it shapes our everyday lives. While in 1995 much of our personal information was stored in filing cabinets held under lock and key, today our smartphones beam personal information to the world every second.



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

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

Summary of key changes



What's changed?

The core rules of data protection remain broadly the same. Anyone familiar with the existing rules and obligations of the Data Protection Act will find GDPR familiar. However, there are a number of important changes and new obligations to be aware of. Plus, the penalties for getting it wrong are much more severe.

Brexit and GDPR

The UK Government has confirmed that GDPR will apply to the UK when it comes into force in 2018.

"We will be members of the EU in 2018 and therefore it would be expected and quite normal for us to opt into the GDPR and then look later at how best we might be able to help British business with data protection while maintaining high levels of protection for members of the public."
Karen Bradley MP, Secretary of State for Culture, Media and Sport

If the UK is to remain a full member of the Single Market, or maintain a close trading relationship along the lines of the EU-Canada Comprehensive Economic and Trade Agreement (CETA), then UK businesses will need to fully abide by the rules set out in GDPR.

"If the UK wants to trade with the Single Market on equal terms we would have to prove 'adequacy' – in other words UK data protection standards would have to be equivalent to the EU's General Data Protection Regulation framework starting in 2018."
Information Commissioner's Office

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 under the GDPR must be justified using one of the following conditions for processing:

If the data is sensitive, 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 sensitive 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 if 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 updated 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.

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.

Consent can be withdrawn at any time and there must be explicit consent given to transfer data outside of the EU.

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:

WRONG

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

RIGHT

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 will no longer be 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 currently obtain consent and assess if 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

Someone can only be contacted for marketing if they have given consent or if there is an existing relationship with them and a similar product or service is being offered. To prove consent has been given, some firms operate a "double opt-in" model. After initial consent is given, an email is sent to 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.

New 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 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.

The Google Spain ruling

In 2014, the European Court of Justice issued a landmark ruling that internet search engines must consider requests from individuals to remove links to web pages that reference their name. Since then, Google and other search engines have published an online form for EU citizens to request removal of links. On its first day of operation, Google received more than 12,000 requests for de-linking.

What to do: Ensure there are procedures for dealing with data portability and right to be forgotten requests

Privacy

Privacy notices, or "how we use your information" guides that are generally given when data is being collected, will have to contain much more information than before. The condition for processing must be included in the privacy notice, as well as the person's rights. 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:

- Consider privacy by design and privacy by default in new and existing applications
- Check and update your privacy notices

Changes for 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.

Unlike many current data protection laws, much of GDPR will also apply directly to data processors. The contracts between controllers and processors will have to include a lot more detail, and processors may also be liable for compensation claims.

If you have contracts with data processors, check if they are compliant with the new Regulations. They may have to be amended and any new contracts with data processors should comply with GDPR.

What to do:

- Review any current or future contracts with data processors

Data Protection Officers

Data Protection Officers are responsible for everything related to keeping data secure in the company. Under GDPR, the role of Data Protection Officers will be strengthened. They will report directly to the highest levels of management and cannot be easily dismissed.

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."

GDPR requires companies that process large amounts or particularly sensitive data to appoint a DPO. This includes companies:

Processing more than **5,000** personal records per year

Employing **250** or more staff

ALL public sector organisations

What to do: Consider if you need to appoint a Data Protection Officer

International data transfers

If you deal with any international transfers of data, then your current data protection policies will likely include some provisions about transferring data abroad, particularly if it is going outside the EEA. GDPR preserves the current rules for international transfers, but enhances them in a few key ways:

EU-US Privacy Shield

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 will designate an 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 will appoint one SA as its "lead authority" based on the main establishment of the business. This "lead authority" will act 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.

Not all of the details of GDPR have been finalised yet. A group known as the Article 29 Working Party is currently writing additional guidance and clarifying points of law before the Regulations come into force. After that, a European Data Protection Board, made up of one member from each supervisory authority, will take a lead role in providing guidance and coordinating enforcement throughout the EU.

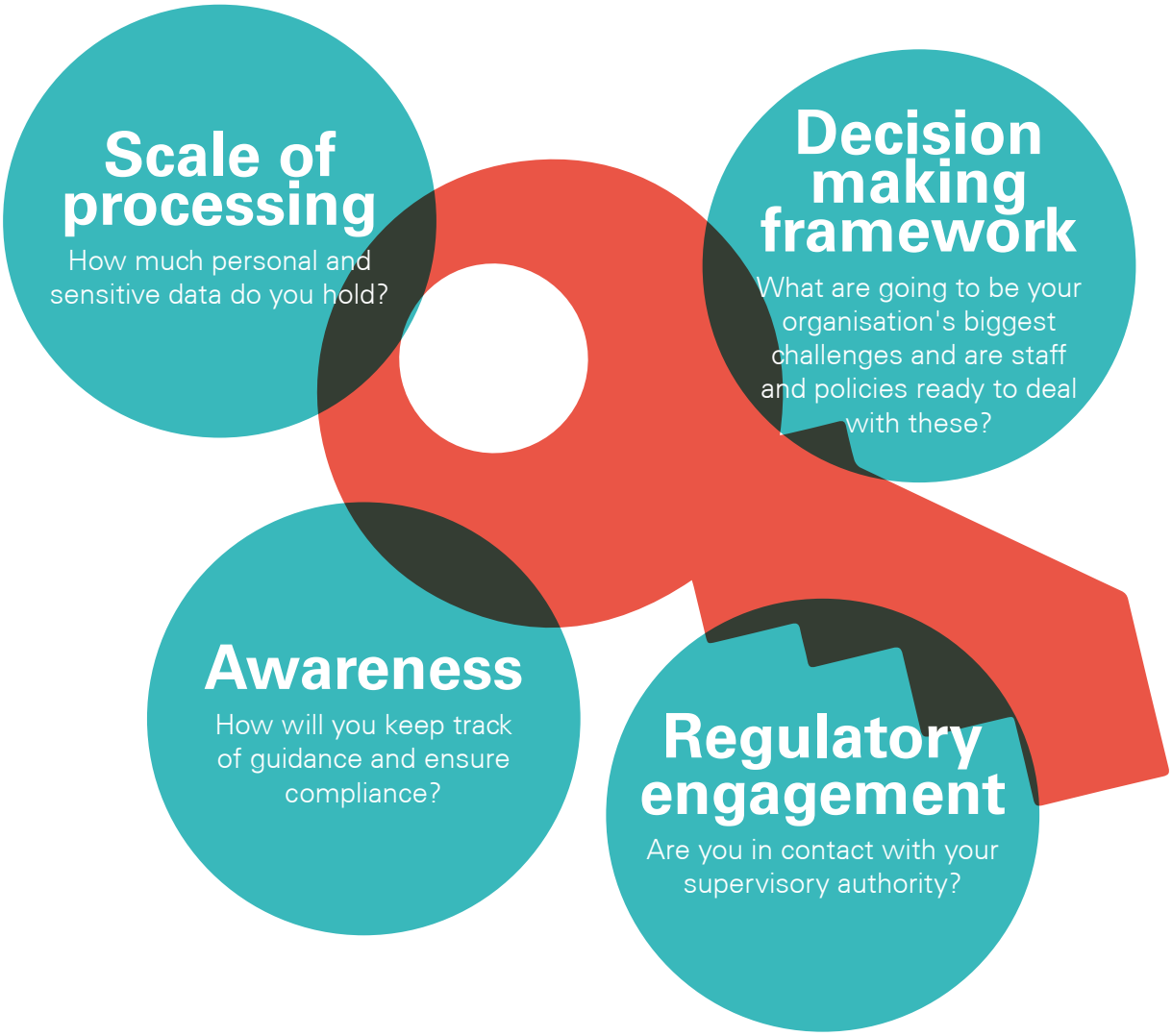
Who is in charge?

Ireland is home to the European headquarters of many major international corporations including Microsoft, Google, Facebook, PayPal, Apple, Yahoo, and more, so it is likely that the Irish supervisory authority (Data Protection Commissioner Ireland) would deal with any major data protection issues for those companies. 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

Balancing risks and regulation will be a difficult process as the new era of GDPR begins. 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 brings in a much stricter 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.

There is a new requirement to report serious or major breaches.

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.

However, 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 would be publicised.

How do I demonstrate compliance?

1 Create 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 staff have adequate and up to date training on data protection and GDPR changes

Preparing for GDPR checklist

Review the ways you currently 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 will be updated in reference to 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 if you need to appoint a Data Protection Officer.

Check 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 may impact 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 have adequate and up to date training on data protection and GDPR changes.

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

Data protection staff awareness training

VinciWorks has developed a new data protection training course, combining the latest in policy and law with best practice guidelines. Users are taken through every step of data protection, with the course specifically tailored for their role in the organisation, with specific modules for HR, IT and marketing departments.

VinciWorks data protection training includes key changes in each area that will happen as a result of GDPR, enabling staff to be uniquely prepared for implementing the necessary changes in their areas.

A special GDPR-focused training module will also be available alongside the comprehensive data protection training to ensure compliance with current and future data protection laws.

http://vinciworks.com/dataprotection

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/corporate-training**

VinciWorks

Innovative risk and compliance solutions

www.vinciworks.com

enquiries@vinciworks.com

+44 (0) 208 815 9308