INTRODUCTION TO GDPR:
THE GENERAL DATA PROTECTION REGULATION

The General Data Protection Regulation (GDPR) is a substantial new law passed down by the EU to replace the Data Protection Act 1998 (and will not be affected by Brexit). It comes into enforcement on May 25, when the local regulator will begin making actions against companies for failing to secure data properly, processing data without proper purposes, or if they fail to properly grant people their rights to control their own data. Much of the regulation is familiar from what was in the Data Protection Act, but a lot has changed.

Client:		Course Date:	

WHAT'S NEW ABOUT GDPR COMPARED TO THE DPA?

Greater emphasis on accountability
Companies have more incentives to get away from consent and rely on other legal bases, which afford more freedom to organisations. But in the return the ICO asks for a lot more in terms of internal governance, reporting, record keeping and demonstrating responsible processing. We've got to put this front and centre of the organisation

Significantly enhanced rights for Data Subjects
The new law hands a lot more power to Data Subjects to access and restrict the use of their data, including the 'Right to Be Forgotten' and for consumers to move information from one company to another with ease.

Much heavier fines
Reaching €20 million and beyond – and no longer just for breaches, but for *non-compliance* alone. The fines are supposed to be 'dissuasive' so they are designed to scare others into compliance by making an example. There are also new legal torts which open companies to litigation when individuals suffer material harm or emotional stress due to misuse of their data.

WHY IS IT IMPORTANT?

It is not an overstatement to say that the GDPR completely transforms what Data Protection means in society.

- It effectively raises our ability to control our data to the status of a human right.
- It has ushered a whole new industry for data protection management and compliance consulting, and is believed to create demand for 30,000 new Data Protection Officer roles.
- Data misuse cases are expected to give rise to a new breed of ambulance chasing similar to the PPI scandal.

The cost of non-compliance is also serious damage to the company's reputation. We protect against these risks by:

- Processing data in a manner our customers would expect
- Reducing the chances of a data breach and knowing how to respond if we think one occurs
  ourselves to handle them
- Being able to properly handle requests from individuals
- Keeping detailed records of our Data Protection activities.

MAJOR CASES WITH SERIOUS FINES:

- **TalkTalk:** Fined £400,000 for security failings (could have been £59m under GDPR).
- **BUPA**: Admitted losing 547,000 customer records.
- **Uber:** Admitted paying hackers a ransom of $100,000 to delete hacked data. (Under GDPR they could be fined £2.8bn).

PRINCIPLES AND RESPONSIBILITIES

The GDPR (with amendments in the Data Protection Bill 2018) places a heavy burden on organisations to ensure they are processing people's data responsibly. The Data Protection Principles guide how all organisations should ensure that all processing activities are:

Specific, Transparent, Authorised, Necessary, up to Date, Relevant, Demonstrative, Secure

Alongside the Principles we have our own Privacy Standard and other Data Protection Policies which guide our approach to minimising the data we use and behaving how Data Subjects would expect.

DATA PROTECTION PRINCIPLES

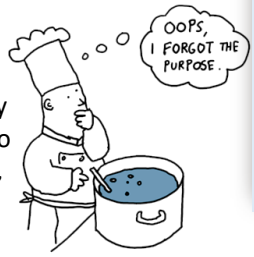
- FAIR, LAWFUL and TRANSPARENT processing
- For SPECIFIED, explicit and legitimate purposes, and not for any use that hasn't been notified to the Data Subject
- RELEVANT to what's necessary for the specified purpose
- ACCURATE and UP-TO-DATE, taking steps to correct inaccuracies.
- Kept only for as long as NECESSARY
- Appropriately SECURED, taking account of likely risks
- To DEMONSTRATE compliance and accountability

Keeping Data Subjects informed

Giving people clear and concise information is key to making data protection transparent, and lets them know that we care about their rights, and we aren't trying to hide anything from them. We give people **Privacy Notices** when we collect their data, keeping them as short and clearly written as possible.

Data minimisation

For the first time, businesses are starting to consider **Data Minimisation** – thinking about if they really need the information they collect. We have to make sure we justify every piece of data we collect, what is our **Legal Basis** for processing the data, the specific **Purpose** and **Retention Period**.



THE BASICS:

SCOPE OF THE LAW: The GDPR only covers personal Data which is processed electronically, or as part of a filing system.

- Data Subject: Any living person (who lives in or comes from the EU)
- Personal Data: Any information relating to an individual that can identify them (also if you combine it with other data)
- Filing System: Includes in an electronic processing, as well as filing cabinets, contact books, indexes, folders, archives – anything you can search to find information.
- Data Controller: An organisation with the ability to make decisions about processing an individual's information.
- Data Processor: An organisation who only processes data on the strict instructions of a **Controller** under contractual obligations.
- Consent: An individual's Freely-given, Unambiguous, Specific, Separate, Indication of wishes and, (in the case of Sensitive data) for an Explicit purpose. All consent forms must be **FUSSI(E).**
- Privacy Notice: An outline of what we do with people's data (including why, how, and for how long) which we must provide to all Data Subjects.

LEGAL BASES FOR PROCESSING

We only process individuals' data when necessary for one of the following:

- To perform a contract
- To comply with legal obligations
- For our legitimate interests;
- To protect someone's vital interests
- For the activities of a public body

Or, if we have the individual's consent.

PROCESS PURPOSES

These can include relationships with customers, to marketing, reporting finances to HMRC, and recruitment – and must be properly justified. Data should only ever be used for the purpose is was collected, so you should never use company data resources for personal reasons, and bear in mind the legal bases for processing.

RETENTION PERIODS

We must make sure we are consistent in how long we retain people's data. This is usually determined by the length of time they are actively engaged with us, plus a reasonable amount of time afterwards to allow for other purposes such as record keeping, tax reporting, and legal claims. The company's **Data Retention Policy** has more information about this.

SPECIAL CATEGORIES OF SENSITIVE DATA

Sex
Politics
Ethnicity
Clinical
Ideology
Associations
Lifestyle

Some kinds of data can only be processed under particular conditions. You should never ask for this kind of data at all unless it is strictly required by an approved processes processing always be sensitive around asking anyone for this kind of data and accept that they may be within their rights not to provide it.

Some employees may process criminal convictions data about staff and applicants – this can only be used for recruitment processes as long as it is done in compliance with out **Processing Sensitive Data Policy**. This has to be given special protection to ensure that any data we process is destroyed once it has been checked. You should have the confidence to tell anyone who refuses to submit basic DBS certificate that we have the legal right to request one from every candidate, and to undertake enhanced checks in certain circumstances, such as a for jobs involving children or vulnerable people.

DATA SUBJECTS' RIGHTS

Your ability to determine the use of your own data has been lifted to the level of a Human Right. People have more control over their data than ever before, and that includes **you**.

These are the most important rights to bear in mind:

Information
Anyone who has your data should have told you by now what they use it for, and any changes to their policies.

Erasure
Any company on the web, or who you object to processing your data must delete you from their system at your request, unless they have compelling reasons that outweigh your rights.

Access (SARs)
Must tell you about their processing provide a copy of all your data they hold. There are very few reasons a company can refuse to fulfil this, and there is no more £10 fee.

Portability
Who holds your data should not hold your back from moving to a different service provider.

Restriction
If you object, you can tell the company only to store your data unless they get your consent.

Objection
Applies to any legitimate interest process and marketing in all circumstances. The Controller must cease processing.

Data Subject requests must usually be fulfilled within one month and any failure could constitute a breach of the law and make the processing unlawful. Individuals also have the right to request any rectification of inaccurate data, and to object to Automated Decision Making (such as credit scores assessed by
a computer, or early recruitment selection based on psychometric tests). Due to the GDPR a lot more people are likely to become aware of their rights so we expect more will actively use them.

SUBJECT ACCESS REQUESTS (SARs)

Any employee can be the point of contact for a SAR, or any other type of Data Subject request – so escalate them to a manager ASAP so the responsible person can follow the correct process. It's important that we properly identify someone before completing their request, and in many cases we may have to refuse, so leave it to the proper authority to make this decision.

WHAT DO THEY LOOK LIKE?

A Subject request can come in the form of an email or a telephone call. The person making them may be disgruntled about something so you need to be careful not to frustrate them further.

- **DO NOT** agree to fulfil a subject request on the phone or attempt to resolve it yourself – outline that there is a policy in place to handle these matters securely.
- If you receive a request that sounds like a SAR, inform a manager or responsible officer immediately – all SARs must be completed within a time limit of one month.
- Politely direct the requester to the relevant officer.
- The proper handling of a request may save us a customer or convert someone to understand we did everything we could to assist them.

WHAT DO TO:

ESCALATE UP TO A MANAGER: We have a procedure in place to handle SARs so make sure the relevant person knows about them ASAP. **DON'T TRY TO RESOLVE THEM YOURSELF.**

EXAMPLES OF A COMPLAINT:

TOO MANY EMAILS: People may wish to make requests about their data if they feel they have been victim of obtrusive marketing or persistent communications. ***There may be an opportunity to help them in another way before going down the route of a SAR, such as taking them off a mailing list or deleting duplicate contacts.***

DISTORTION OF LEGAL CLAIMS: Someone considering legal action against the company may try to order us to erase their data prior to making the claim so we are less prepared to defend ourselves in court. ***The law protects us from having to delete information which we keep for employment or contract purposes.***

DISGRUNTLED CUSTOMER: There is likely to be something else the requester is angry about and they are using their data rights to punish us. ***Try to find out what is really bothering them and whether they have an ulterior reason for contacting us.***

DATA BREACHES:

The biggest threat the company faces is from a Data Breach, defined as any unauthorised access, disclosure, loss damage or destruction of personal data. A Data Breach poses a number of risks to the individuals we work with, and to us as a Data Controller:

- Loss of systems required to conduct our business
- Hacked data may expose individuals to identity theft
- Financial liabilities if the breach has a material affect on the Data Subject
- Loss of reputation if we have to report our breach to the ICO and our customers.

Any employee can be the first point of contact for a Data Breach, so you need to know how to spot them and what to do

71% of security breaches hit small businesses

65% of large firms detect at least one data breach a year

1/5 SMEs trained staff in data security in 2016

815 data security incidents reported to the ICO in Q3 2017

11% of total data breaches involve a cyber threat (ICO)

Cyber-criminals:

- Steal credentials to send legitimate looking emails to other companies.
- Target small organisations who may have laxer security and typically pay out to resolve ransom-ware attacks.

WE PROTECT OURSELVES BY:

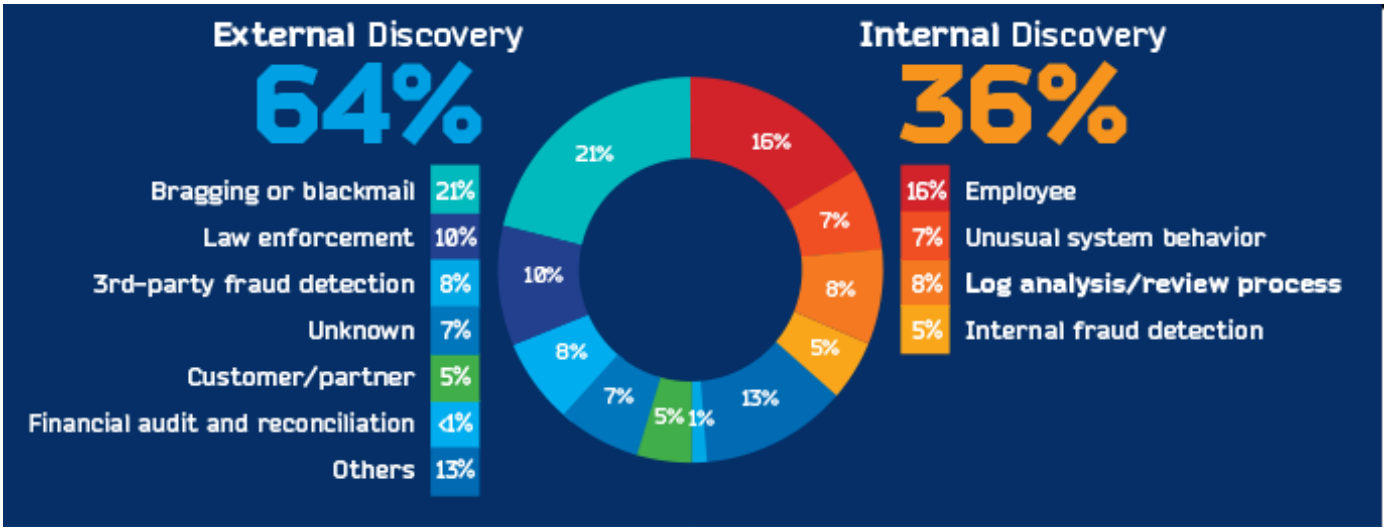
Providing company devices: These give appropriate staff adequate security when working remotely.
Restricting systems access: The company has to draw distinctions across which staff can access what data. You should only have access to data that's necessary for your role. If this is not the case alert your manager.
Preparing our team: Staff can often be the weakest link in security, so we are going to keep you updated on cyber-security threats so you know what to look out for.

Key Cyber Threats:

- 1 in 5 data breaches are caused by malware or malicious WiFi
- Allowing BYOD significantly raises the chance of a breach
- Phishing scams are still the most common cyber-security threat – involving a malicious email disguised as an official sender.

EXAMPLES OF A DATA BREACH:

- Sharing passwords with colleagues.
- Opening email malware.
- Accidentally deleting data.
- Losing company equipment
- Making copies of company data for own use.
- Accidentally sending email to the wrong recipient.
- Sending group emails revealing their email addresses to each other.
- Disclosing information to someone over the phone.
- Losing paper records to fire or flood.



Source: ObserveIT

SECURITY

The company has a host of updated security policies to adapt our activities to the new law. Strong security measures are crucial because they:

- Ensure our data processing is always lawful and can't be criticised
- Take steps to **prevent** data breaches
- Protect the rights of individuals
- Demonstrate our commitment to Data Protection

Crucial to avoiding data breaches is to take as many preventative steps as we can.

Strong passwords: If there isn't a system requiring you to change your password regularly you should do this yourself, and create a new password with a mixture of uppercase and lowercase letters, numbers and symbols.

Be alert to visitors: Anyone wandering into the building may have accidental access to any number of files on desks so it is our policy now to ensure that any visitor the building is accompanies at all times.

Leaving your desk unaccompanied: Take care not to leave any information containing personal data open to others when leaving your desk. Lock away files when not in use and log off your computer when going out of the office.

Stick to company systems: Staff who maybe keeping their own contact sheets or compiling other forms of data outside the company system may be in breach of new policies so ensure you no longer do this if so. If you take personal data from the company without authorisation this is a criminal offence, not to mention a breach of company policies.

Check and double check people's details: When you take down someone's personal information, ask them to send you a contact card, read their details to them on the phone, or ask them to proofread a form they've filled in. The most common cause of a data breach is that information was sent to the wrong email address by mistake, because someone took down the address incorrectly.

Don't send messages on social media: It is the company's policy now to only use email servers and apps on company mobiles (like WhatsApp) to contact clients and workers – it's necessary that any data which is used for work is kept in a form which the company can control, so we ask you not to use any form of communication that it can't access.

Report unsolicited emails / calls / messages: Do not act upon them without authorisation and until their validity has been checked.

Transferring Information: You should never transfer personal data to anyone until you have permission and are sure it is within the company's **process purposes**. Avoid sending files as email attachment. Email is particularly vulnerable to attack. Send documents by using an FTP client / cloud service. If not an option, and you have to send by email use a password-protected document and send the password by text.

Don't deal with situations on your own: If you open a malware link in an email or lose your company mobile, don't try to brush it under the carpet or solve the situation yourself. There is always a solution to protect data either by reverting to back-up or remotely encrypting or wiping devices but it must be handled by the responsible officer.

NEW COMPANY POLICIES

The company has a range of new policies in place to prepare for the changes in law, many of which will affect how you work from now on.

Privacy Standard – The overarching standard by which the company now operates and which guides the writing of all other data policies.
Data Security Policy: Employee Code of Conduct – Rules for employees to abide by in their work
Data Protection: Retention Policy – Informs us how long we can keep data and when we need to be purging our systems.
Data Protection: Legal Basis for Processing Policy – informs us what justification we have for processing specific kinds of data, and when we need to use consent.
Various privacy notices for employees, workers, clients, online users – a bundle of different privacy notices, which we must legally provide at the point of any collection of personal data.

EMPLOYEE RIGHTS

You are a Data Subject as well, and the company processes your data similarly to everyone else it comes into contact with. You need to make yourself familiar with the Company's policies about processing your data and if you haven't seen a Privacy Notice or signed a consent form for something, speak up.

Employers have a responsibility to their staff, just as much as their customers when it comes to data.

- Due to the nature of the employer-employee relationship, there are very few circumstances where it is justified to ask an employee to consent to any kind of data processing, so this will only happen in very rare occasions and won't affect your employment.

DEMONSTRATING COMPLIANCE

An important consideration for managers and supervisors is to make sure they take every possible opportunity to record all activities around data protection – from logging SARs to seeking advice, conducting meetings and reviewing policies. You should have the procedures in place to monitor your own compliance and be able to demonstrate your efforts to the ICO whenever the need arises. It takes just one data breach to put the company on their radar, which could result in an audit, investigation, or various kinds of orders. That means that staff must always:

- Take opportunities to log any activity around Data Protection procedures.
- Ensure that the right officers are alerted to any potential data breach or Data Subject request quickly.

Below are the three main resources for keeping records of compliance.

REGULAR BOARD MEETINGS

- **Log internal developments:** Record changes being made in the organisation to show the attitude taken.
- **Make suggestions:** Keep a look out for opportunities to improve data protection procedures and raise them with your department head to escalate.

BREACH / SAR LOGS

- **Procedures to trace the process from start to finish:** Escalate them to a manager ASAP so the responsible person can follow the correct process.
- **Record everything:** All near misses as well for demonstration purposes.

INFORMATION ASSET REGISTRY

- **Records processing activities:** Demonstrates the company gives careful consideration to the data we process and attempts to minimise we can.
- **Informs our activities:** Guides the business on our legal bases and retention periods
- **Keep up-to-date:** Add any new kinds of processing.