INTRODUCTION TO GDPR:
THE GENERAL DATA PROTECTION REGULATION

The General Data Protection Regulation (GDPR) imposes significant additional requirements on those who process personal data and enhances data subjects' rights. Together with the Data Protection Bill (expected to be the Data Protection Act 2018) it replaces the Data Protection Act 1998 (DPA).

The new rules take effect on 25th May 2018 at which time the Information Commissioner's Office (ICO) will begin taking action against organisations who fail to secure data properly, process data without proper justification, or who fail to comply with the new rights.

Client:	Scattergoods Agency Ltd	Course Date:	28th April 2018

WHAT'S NEW ABOUT GDPR COMPARED TO THE DPA?

Greater emphasis on accountability
Organisations can no longer rely on consent by default and will often have to rely on other legal bases to justify their processing activities. The ICO now requires a lot more internal governance, reporting, record keeping and demonstration of responsible processing. Practices and processes to support our compliance must now be 'front and centre' of our activities.

Significantly enhanced rights for Data Subjects
The new law hands a lot more power to individuals whose data is processed ('data subjects') to access and restrict the use of their data, including the 'right to be forgotten' and for data subjects to move information from one company to another with ease (known as the 'right to portability').

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 setting an example. Data subjects call also sue organisations directly and recover compensation.

WHY IS IT IMPORTANT?

It is no overstatement to say that the GDPR completely transforms what Data Protection means in our society.

- It effectively raises data protection to the status of a human right.
- It has created a 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 claims industry.

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

- Processing data in a manner data subjects would expect
- Reducing the chances of a data breach and knowing how to respond if we think one has occurred
- Being able to properly handle requests from data subjects
- Keeping detailed records of our data processing 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 new data protection legislation places a heavy burden on organisations to ensure they are processing data responsibly. The Data Protection Principles guide how all organisations process data and requires that all processing activities are:

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

These principles are reflected in our new policies which explain our approach to compliance.

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
- **DEMONSTRATING** 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, and make these as short and clearly written as possible.

Data Minimisation

Organisations now need to focus more on minimising their Data– thinking about if they really need the information they collect. We have to ensure we justify all personal data we collect: what our **Legal Basis** is for processing the data, the specific **Purpose** and appropriate **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 (or can do so if you combine it with other data)
- **Filing System:** Includes 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 that processes data on the instructions of a **Controller and** under contractual obligations
- **Consent:** An individual's **F**reely-given, **U**nambiguous, **S**pecific, **S**eparate, **I**ndication of wishes and, (in the case of Sensitive data) for an **E**xplicit purpose. All consent forms must be **FUSSI(E).**
- **Privacy Notice:** An outline of what we do with data (including why, how, and for how long we process it) 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 such things as managing relationships with customers, marketing, financial management and recruitment – and must be properly justified. Personal data should only ever be used for the purpose is was collected, so you should never use the organisation's data resources for personal reasons, and always be mindful of the purpose and treat the data consistently with this.

RETENTION PERIODS

We must make sure we are consistent in how long we retain personal data. This is usually determined by the length of time the data subject is 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.

Sex
Politics
Ethnicity
Clinical
Ideology
Associations
Lifestyle

SPECIAL CATEGORIES OF SENSITIVE DATA

Some kinds of data can only be processed under particular conditions. You should never collect or use this kind of data unless it is strictly required by an approved process. 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 complies with our **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. We must undertake enhanced checks in certain circumstances, such as a for jobs involving children or vulnerable people, however, we should not require criminal records data by default.

DATA SUBJECTS' RIGHTS

Data subjects have more control over their data than ever before, and that includes **you**.

These are the most important rights to consider:

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

Erasure
If you object to your personal data being processed you can order the controller to delete it, unless they have compelling reasons that outweigh your rights and freedoms.

Access (SARs)
You must be given a copy of the data they hold upon request. There are very few reasons a company can refuse this, and they can no longer charge for this.

Portability
If you provided the data and it is processed under consent or contract, you can require it to be transferred elsewhere.

Restriction
In some circumstances you can insist that your data is stored by not processed until you give your consent.

Objection
You can object to processing and require the controller to re-assess their legitimate interest assessment.

Individuals also have the right to request that inaccurate or incomplete data is corrected, and to object to automated decision making (such as credit scores assessed by a computer, or early recruitment selection based on psychometric tests).

Requests to exercise these rights should be addressed within one month from receipt, and failure to do so may constitute a breach of the law and make processing unlawful.

As time goes on, a lot more people will become aware of their rights and choose to exercise them.

SUBJECT ACCESS REQUESTS (SAR)

These *should* go to a designated email address, but they *may* come to you directly – so be alive to this possibility and escalate any request to a Responsible Person without delay.

It's important that we properly identify the data subject before complying with a request, and in some cases we may have to refuse the request, so leave it to the Responsible Person to deal with the request and make these decisions.

WHAT DO THEY LOOK LIKE?

A request can come in an email or a telephone call. The person making them may be aggravated or upset about something so be careful to treat them with respect and avoid aggravating them further.

- **DO NOT** agree to fulfil a 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 Responsible Person immediately – all SARs must be completed within a time limit of one month
- The proper handling of a request may save the relationship or satisfy the person that we are handling their data properly.

WHAT DO TO:

PASS TO A RESPONSIBLE PERSON: We have a procedure in place to handle SARs so you must escalate requests without delay.

DON'T TRY TO RESOLVE IT YOURSELF.

EXAMPLES OF A COMPLAINT:

TOO MANY EMAILS: People may wish to make requests about their data if they feel they have been a victim of intrusive 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 need for these purposes.***

DISGRUNTLED INDIVIDUALS: 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:

A data breach is any unauthorised access to, disclosure of, loss of, damage to, or destruction of, personal data.

A Data Breach can cause a number of serious risks to our data subjects, 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 effect on the data subject
- Loss of reputation if we have to report our breach to the ICO and our customers

Any employee may be the first person to learn of a possible 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

Cyber-criminals:

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

WE PROTECT OURSELVES BY:

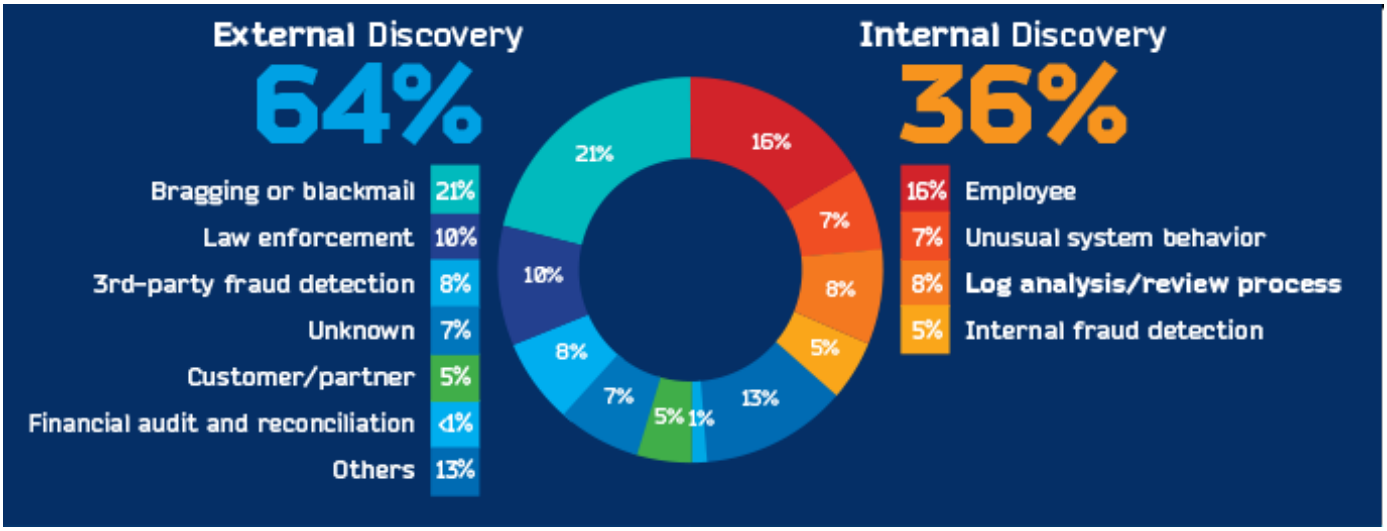
Providing company devices: These give appropriate staff adequate security when working remotely
Restricting systems access: We make careful decisions about which staff can access what data. You should only have access to data that's necessary for your role. If this is not the case alert your manager.
Preparing our team: Human error can be a weak 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
Allowing employees to use their own devices 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:

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 organisation has new security rules 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

It is crucial that we take as many preventative steps as we can to avoid data breaches.

Strong passwords: If there isn't a system requiring you to change your password regularly you should do this yourself. Always use passwords 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 accompanied 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 keep their own contact lists or compile other forms of data outside the approved systems may be in breach of the new policies. If anyone takes personal data from the company without authorisation this can result in prosecution and gross misconduct dismissal.

Check and double check people's details: When you take down someone's personal information make sure you double check it. The most common cause of a data breach is information sent to the wrong email address by mistake.

Don't send messages on social media: It is the company's policy to only use company devices for communicating with contact clients and workers – it's necessary that any data which is used for work is kept in a form which the organisation can control, so we ask you not to use any form of communication that we 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 sensitive documents to anyone until you have permission and are sure you are authorised to do so. Avoid sending files as email attachments, which are particularly vulnerable to attack. Send sensitive documents by using an FTP client such as dropbox of Google Drive. If 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 often 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 – Rules for employees to abide by in their work.
Data Retention Policy & Schedule – Informs us how long we keep our data and when we need to purge our systems.
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, etc – these must be provided to the data subjects

EMPLOYEE RIGHTS

You are a Data Subject and the organisation applies the same high standards to your data as it does to all other data subjects.
You need to make yourself familiar with the Company's policies about processing your data.
If you haven't seen a Privacy Notice in the near future 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.

DEMONSTRATING COMPLIANCE

An important consideration for managers and supervisors is to make sure they take appropriate steps to record all activities around data protection.

It takes just one data breach to put the company on the ICO's radar, which could result in an audit, investigation, or various kinds of orders. This means that staff must always:

- log actions in response to data subjects' right and data breaches
- Ensure that a Responsible Person are alerted to any potential data breach or data subject request quickly.

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

MEETINGS

Information sharing: make sure you inform your manager about any new practice or requirement that relates to personal data
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 these to a Responsible Person ASAP so they can follow the correct process.
Record everything: including all near misses.

INFORMATION ASSET REGISTRY

Records processing activities: Demonstrates the company gives careful consideration to the data we process and attempts to minimise if we can.