The new rules

GDPR (General Data Protection Regulations) is Europe's new framework for data protection laws. It goes live on 25th May 2018.

The rules introduce new rights for people to access the information companies hold about them, obligations for better data management for businesses, and a new regime of fines. The rules have come about as a result of some very public breaches of personal data security at Yahoo, Google, Facebook & Morrisons!

Casey will be more accountable for our handling of people's personal information. This can include having data protection policies, data protection impact assessments and having relevant documents on how data is processed.

Under GDPR there's a need to have documentation of why people's information is being collected and processed, descriptions of the information that's held, how long it's being kept for and descriptions of technical security measures in place.

As well putting new obligations on the companies and organisations collecting personal data, the GDPR also gives individuals a lot more power to access the information that's held about them. When someone asks a business for their data, they must stump up the information within one month. Everyone will have the right to get confirmation that an organisation has information about them, access to this information and any other supplementary information.

One of the biggest, and most talked about, elements of the GDPR is the power for regulators to fine businesses that don't comply with it. If an organisation doesn't process an individual's data in the correct way, it can be fined. If there's a security breach, it can be fined.

What data is covered?

GDPR requires companies to identify all “Personal Data” which it processes
Personal data is any data that enables the identification of a “Natural Person”. A “Natural Person” is an individual human being.

In addition Personally identifiable information (PII), or sensitive personal information (SPI), as used in information security and privacy laws, is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context.

Examples of personal data are:-

1. Full and Last name
2. Personal Email address
3. Business email address
4. Personal telephone number
5. Date of birth
6. Next of kin information
7. National Insurance Number
8. Educational Information
9. Passport
10. Payroll Information
11. Employment History
12. Photograph
13. Mother's maiden name
14. Work based performance information

What does this mean for Casey?

The company must identify all personal data that the business processes and identify the basis on which it does so. [Note: processing includes storage]

The main sources of personal data in Casey are as follows (non-exhaustive):-

- Employees
- Unincorporated customers
- Residents (client tenants)
- Casey tenants
- Unincorporated suppliers/subcontractors
- The general public

Casey is required to identify the basis on which it processes. The permitted bases are detailed below;

1. **Consent**—The individual has given the organisation clear consent to process their personal data for a specific purpose.

2. **Contract**—The data processing is necessary for a contract with the individual, or because they asked for specific steps before entering into a contract.

3. **Legal obligation**—The data processing is necessary for the organisation to comply with the law—not including contractual obligations.

4. **Vital interests**—The data processing is necessary for the organisation to protect an individual's life.

5. **Public task**—The data processing is necessary to perform a task in the public's interest or for the organisation's official functions, and the task or function has a clear basis in law.

6. **Legitimate interests**—The data processing is necessary for the organisation's legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data that overrides those legitimate interests. (Note: This cannot apply if the organisation is a public authority processing data to perform own official tasks.)

Although Casey may have a legitimate basis on which to process the personal data, it is still required to take all necessary steps to protect this data, to centralise and control its storage and to record its location.

Should the company receive a "subject access request", the ability of the company to provide details of the data held within the deadlines required will be dependent on this storage and locational recording.

Procedures

To ensure compliance with GDPR the Group will adapt and expand its procedures and data storage facilities.

Meetings with relevant staff have been held to explore existing and proposed processes with respect to data protection and the requirements of GDPR.

New/Amended procedures regarding the use of email, mobile phones, Health and Safety, client resident information, suppliers and employees, will be issued and communicated to employees as appropriate.

3rd Party Processors

Where necessary Casey will share personal data with 3rd parties. If this is required, data will be shared securely and we will require 3rd party processors to confirm full compliance with GDPR themselves.

Client Data

Casey has received correspondence from clients requesting confirmation from the company of its GDPR compliance, its policy and its adherence to the clients requirements regarding personal data.

These requests include;

- Confirmation that personal data will only shared with "reliable" persons
- That those persons are trained in GDPR, confidentiality, security and the care of personal data
- That we obtain consent from the client before data is shared with 3rd parties
- That all personal data will be returned or deleted when the contract is "terminated"
- That we report any security breaches to the client immediately

All client requirements will be saved within a folder on the company K Drive under General Information/GDPR/Client requirements.

It is up to the relevant staff (whether this be business development or delivery teams) to make themselves aware of and to ensure compliance with client requirements. These client requirements should be discussed in the tender handover meeting, the permission to proceed meeting and in the internal pre-contract meeting.

Data from the General Public

As a largely business to business organisation (B2B), Casey doesn't have the same level of interaction with the general public as business to customer (B2C) businesses. However, any interaction with members of the public should observe the same level of rigorous care with data protection.

Wherever possible, the obtaining of personal data for members of the public should be kept to the very minimum.

Non-Corporate customers

On the rare occasions that Casey has non-corporate customers, only data required to credit reference the customer, to invoice and to collect any debt should be obtained [this excludes credit card sales which have their own personal data protocol].

If the sale to the customer is within the waste management business, then additional data which is required to assess the waste and meet EA and HMRC requirements should be retained in the appropriate secure storage.

Customer information should be stored in secure locations such as within Dynamics AX/Gatehouse IT systems and in appropriate restricted access folders on the head office network.

Customer account personal data where we have not transacted since 31/07/13 is being deleted unless required for legitimate purposes.

Non-Corporate Suppliers

Casey uses a wide variety of suppliers, consultants, agencies and subcontractors. Although most of these are businesses and therefore not "natural persons", they may still provide contact details to us to aid communication. These should always be business contact details and any personal contact details, if required, should be stored securely.
Where the Group sources supply/services from natural persons, personal data should be kept to a minimum and restricted to only those details that the Group requires for its legitimate interests, legal compliance and contractual obligations.

Training

Casey has already conducted GDPR review sessions with Contracts/Project managers and TLOs and will provide appropriate training to employees regarding data protection and GDPR, via in-house sessions and tool-box talks.

Until this training is undertaken however, employees should at all times be vigilant and alert appropriate authorised personnel to any personal data that is not stored securely. (see Casey GDPR: Employee Personal Data Awareness)

Subject Access Requests & Data rectification

Under GDPR, individuals will have the right to request:

1. confirmation that their data is being processed;
2. access to their personal data; and
3. other supplementary information – this largely corresponds to the information that should be provided in a privacy notice

These are similar to existing subject access rights under the Data Protection Act.

GDPR clarifies that the reason for allowing individuals to access their personal data is so that they are aware of and can verify the lawfulness of the processing.

Any subject access request will generate a response from the company and the company will verify the identity of the person making the request, using reasonable means.

Individuals are entitled to have personal data rectified if it is inaccurate or incomplete.

If Casey has disclosed the personal data in question to third parties, we will inform them of the necessary rectification where possible. Casey will also inform the individuals about the third parties to whom the data has been disclosed where appropriate.

Destruction/Erasure of Data

The right to erasure does not provide an absolute 'right to be forgotten'. Individuals have a right to have personal data erased and to prevent processing in specific circumstances:

1. Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
2. When the individual withdraws consent.
3. When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
4. The personal data was unlawfully processed (i.e. otherwise in breach of GDPR).
5. The personal data has to be erased in order to comply with a legal obligation.
6. The personal data is processed in relation to the offer of information society services to a child.

Under the Data Protection Act, the right to erasure is limited to processing that causes unwarranted and substantial damage or distress. Under GDPR, this threshold is not present. However, if the processing does cause damage or distress, this is likely to make the case for erasure stronger.

There are some specific circumstances where the right to erasure does not apply, where the personal data is processed for the following reasons:

1. to exercise the right of freedom of expression and information;
2. to comply with a legal obligation or for the performance of a public interest task or exercise of official authority;
3. for public health purposes in the public interest;
4. archiving purposes in the public interest, scientific research historical research or statistical purposes;
5. the exercise or defence of legal claims.

Data Breaches

The GDPR introduces a duty on all organisations to report certain types of data breach to the relevant supervisory authority, and in some cases to the individuals affected.

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data.

Notification of a breach is required where the breach is likely to result in a risk to the rights and freedoms of individuals. If unaddressed such a breach is likely to have a significant detrimental effect on individuals – for example, result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

For example, notification would be required to the relevant supervisory authority about a loss of customer details where the breach leaves individuals open to identity theft. On the other hand, the loss or inappropriate alteration of a staff telephone list, for example, would not normally meet this threshold.

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, Casey must notify those concerned directly.