GDPR Action Plan

GDPR – What's New? Key Changes in GDPR

Being more transparent with individuals – customers, customer leads, potential customers, prospects and employees

GDPR requires you to give individuals more information at the time their data is collected. This includes explaining the legal basis of your processing, your data retention periods and that individuals have the right to complain to the Information Commissioner's Office (ICO)

Actions to take now:

- Review your customer terms
- Update your privacy policy
- Individuals (your customer and potential customers) need access to your privacy policy so they can read it (you can include a link on emails, invoices, etc)
- Conduct a Data Audit so that you know what personal data you are currently holding. (Many of you have already done this.) If you have not conducted one, now is the time to do so.
    - With this Data Audit, you should look at and record:
        - What personal data you hold
        - Why do you hold it
        - From whom it was received
        - Where is it kept
        - How long have you been holding it
        - Who do you share it with
        - If consents have been obtained whether those consents are still valid
        - If other lawful basis is used
        - What is the most appropriate lawful basis

- If you are relying on customer consent to legitimise your processing (for example, for email marketing), check that the method of obtaining consent will meet the new rules. Consent requires a positive opt-in.
- If you cannot rely on consent, establish if you can rely on one of the alternative conditions for processing data. These include:
    - Legitimate Interest
    - Contractual requirement
    - Consent
    - Legal obligation
    - Vital interests
    - Public task

Having read and studied the options and the required lawful basis for processing customer's data here at Borsdane Wood Ltd/Dairydata we have decided on:

Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

What is the 'legitimate interests' basis?

Article 6(1)(f) gives you a lawful basis for processing where:

"processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."

This can be broken down into a three-part test:

Purpose test: are you pursuing a legitimate interest?

Necessity test: is the processing necessary for that purpose?

Balancing test: do the individual's interests override the legitimate interest?

A wide range of interests may be legitimate interests. They can be your own interests or the interests of third parties, and commercial interests as well as wider societal benefits. They may be compelling or trivial, but trivial interests may be more easily overridden in the balancing test.

The GDPR specifically mentions use of client or employee data, marketing, fraud prevention, intra-group transfers, or IT security as potential legitimate interests, but this is not an exhaustive list. It also says that you have a legitimate interest in disclosing information about possible criminal acts or security threats to the authorities.

'Necessary' means that the processing must be a targeted and proportionate way of achieving your purpose. You cannot rely on legitimate interests if there is another reasonable and less intrusive way to achieve the same result.

You must balance your interests against the individual's interests. In particular, if they would not reasonably expect you to use data in that way, or it would cause them unwarranted harm, their interests are likely to override yours. However, your interests do not always have to align with the individual's interests. If there is a conflict, your interests can still prevail as long as there is a clear justification for the impact on the individual.

Demonstrating your compliance

One of the most significant changes and the overarching theme of GDPR is the principle of 'accountability'. There are new requirements on data processors (you) to demonstrate your compliance by fully documenting all data-processing activities. Fortunately, they are limited for business with fewer than 250 employees.

Actions to take now:

- Consider what records you keep of your processing activities.
- Can you, for example demonstrate your compliance by pointing to your data audit, records, decision making process and actions taken?
- Are you suitably protected if there is a breach?

Mandatory breach notifications

You have no more than 72 hours to report any data protection breach to the ICO. Where this breach is likely to result in a high risk to individuals you must also notify these people with no undue delay.

Actions to take now:

- Ensure you can meet the above timeframes.
- Invest in and use secure systems that include the use of passwords, encryptions, firewalls and anti-virus software. Ensure all are up to date and current.
- Learn how to minimise the risk from hacking, phishing links and emails and other cyber security breaches.

Much higher penalties when things go wrong

Businesses will now face much higher penalties for non-compliance.

Actions to take now:

- Ensure the risk of penalties is fully understood! Visit the ICO Website

Enhanced rights for individuals

As well as subject access rights to their data, individuals will now have the right to receive their data (if they ask what data you hold on them) in a commonly-used and readable format. They also have the right to have their data erased (called the 'right to be forgotten'). This right to erasure is subject to certain exceptions which includes if we have a legal obligation to hang on to certain detail.

Actions to take now:

- Review your process for responding to subject access requests where a person is entitled to request details of the personal information you hold about them.
- Ensure you can supply above without delay, free of charge and in any event within one month.
- Remember that it is already a general principle of data protection law that personal data should be accurate, kept updated and not held for longer than necessary.
- If the individual stops being a customer we suggest deleting all data after one year from cessation, expect for any legal requirement element.

Direct obligations on data processors

There are now direct obligations on data processors (you) such as taking security measures to protect personal data, amongst others, including subcontracts with third parties.

Actions to take now:

- List all your arrangements with data processors such as:
    - Outsourced services and cloud suppliers
    - Businesses that manage your email marketing, e-shots etc.
    - IT service providers
- Ensure they all comply with the new law.

If you have employees

Actions to take now:

- They will need a privacy policy (from you to them).
- You will need to train them in GDPR as presumably they have access to customer data.

To summarise and create a to-do-list. We suggest the following:

1. Set aside some time to become compliant and GDPR ready.
2. Visit the IOC Website for further information.
3. Provide customers with access to your privacy policy, this should be on your website.
4. Record your actions to demonstrate compliance.
5. Check with any third-party provider that uses or has access to your customer's data that they are GDPR compliant.
6. Ensure all digital data is protected, safe and secure via the use of passwords, encryptions, firewalls and anti-virus software. Ensure all are up to date and current.
7. Ensure that **anyone** that has access to your customer's data is fully aware of their responsibilities and trained to do so.
8. Keep all paper data secure and safe. Consider what it going out and about with you, keep to a minimum, and keep secure. Review what is required for the day.
9. Ensure that for marketing purposes you have obtained the correct opt in consents. Re-gain these consents, if required. You will need a record of these new opt in consents.
10. Ensure you are suitably protected from a data breach.
11. Ensure that after one year you delete all old customer data (this is a suggested timeframe)
12. Sign and return form on Page 1 by June 1st 2018.