Rutland County Council

General Data Protection Regulations (GDPR) Awareness for Small Businesses

Adele Wylie - Head of Legal and Corporate Governance

disability confident EMPLOYER

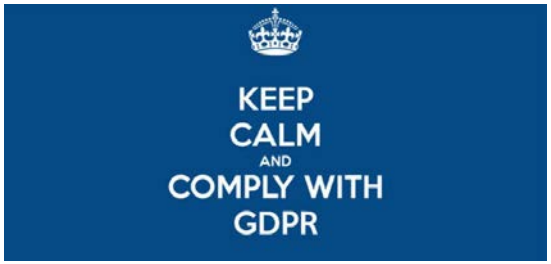
Rutland County Council

Better Rules for Small Business

Stronger rules on data protection called General Data Protection Regulations (GDPR) are being introduced from 25 May 2018. This means citizens have more control over their data and business benefits from a level playing field. One set of rules for all companies operating in the EU, wherever they are based. Find out what this means for your Small and medium-sized enterprises.

(**small and medium-sized enterprises** (SMEs) is made up of **enterprises** which employ fewer than 250 persons)

Act now!



Rutland County Council

Why Change the Rules?

It's about trust...

A lack of trust in old data protection rules held back the digital economy and quite possibly your business.

Only15%...

of people feel they have complete control over the information they provide online.

And helping business boom...

One set of rules for all companies processing data in the EU

Doing business just got easier and fairer

The new system keeps costs down and will help business grow

The Regulator

Information Commissioner's Office role is to uphold information rights in the public interest.

There are a number of tools available to the Information Commissioner's Office for taking action to change the behaviour of organisations and individuals that collect, use and keep personal information.

These include:

- criminal prosecution
- non-criminal enforcement and audit
- Monetary penalty notice on a data controller

What data does GDPR apply to?

You'll need to demonstrate an understanding of the types of personal data and sensitive data (for example health details or religious views) you hold, where they're coming from, where they're going and how you're using that data

- Name
- Address
- Localisation
- Online identifier
- Health information
- Income
- Cultural profile
- and more

Rutland County Council

Let’s go back to basics

- The GDPR will apply to data ‘controllers’ and ‘processors’.
- **Processing**- defined as any operation performed on personal data, such as storing, collecting, recording, organising, sharing, erasure, consulting, etc.
- **Controlling-** determines the purposes for which and the manner in which any personal data are, or are to be, processed.
- A controller will always be a data processor too, but they will also decide the purpose of the data processing activities.

Rutland County Council

The Data Protection Principles

Set out the Main responsibilities for organisations:

1. Processed lawfully, fairly and in a transparent manner in relation to individuals
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. Accurate and, where necessary, kept up to date;
5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
6. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Rutland County Council

Does GDPR apply to my business?

- GDPR applies to any business that processes the personal data of EU citizens.

1. how often does your business deal with **personal data**? This includes your customer data, supplier data? Past and present employees? Anything else?

2. If you're collecting any of this data routinely, you'll need to comply with the GDPR, whether the data is on a spreadsheet, on your computer network, your mobile phone, or in the cloud.

3. Does your business currently falls under the DPA. If so, the ICO has confirmed that the GDPR will apply to you, but remember, the GDPR is much stricter than the DPA.

Rutland County Council

What does your business need to do?

Rutland County Council

1. Know your data

Make sure that you understand;

- What personal data you hold
- Where its coming from
- Make sure that you understand
- where its going
- how you're using that data

Rutland County Council

2. Are you relying on consent?

- Customer or individual ‘consent’ has been redefined and become much tighter, as a result. You need to change the way you seek consent.

DO NOT

- Hide requests for consent in small print
- Have pre-ticked boxes
- Use inactivity as a legitimate way to confirm consent.

DO

- Present consent clearly, and separately to other policies on your website or communications
- Get positive consent to process data
- Check age limit for parental consent

Rutland County Council

3. How are your policies and security measures?

- Look hard at your security measures and policies. You'll need to update these to be GDPR-compliant
- If you don't currently have any, you should get them in place.
- Broad use of encryption could be a good way to reduce the likelihood of a big penalty in the event of a breach.

Rutland County Council

4. Conduct due diligence on your supply chain

- You should ensure that all suppliers and contractors are GDPR-compliant to avoid being impacted by any breaches and consequent penalties.

- You could ask suppliers and contractors to confirm the security measures they have in place, or you could conduct an on-site visit. If their existing measures aren't sufficient, you should review your relationship to ensure they are compliant with GDPR.

- Where your suppliers (as processors) are processing personal data on your behalf (as a controller), you have an obligation to update your contracts with them to include a number of mandatory clauses that can be found in Article 28(3) of the GDPR. These ensure that processors are contractually obliged to provide GDPR-compliant data protection standards.

Rutland County Council

5. Dispose of old data

- One of the key principles of GDPR is to require companies not to hold on to personal data for longer than necessary, or process it for purposes that the individual isn't aware of. Identifying your data categories – what personal data you have, and why – will be very helpful in ensuring you're compliant with the GDPR

Rutland County Council

6. Are your staff aware of GDPR?

- Train your employees if applicable, do they know what they can send, collect, store?

- Ensure your employees understand what constitutes a personal data breach and what the process will be.

7. Create Fair Processing Notices

- This will give people clear information about what you're doing with their personal data

What should it include?

- why you're processing their personal data (the purpose), including the legal basis you have, such as consent

- the categories of recipients you may be sending the personal data to (customer, employee, supplier, etc)

- how long you'll be holding onto the data (the 'retention' period'), or the criteria used to determine these time periods

- You'll also need to notify individuals of the existence of their personal data rights

Rutland County Council

8. Do I need a Data Protection Officer?

- If you employ fewer than 250 people- no
- Being a small business doesn't mean you fall out of the GDPR scope, even if you don't need to employ a DPO. It's recognised that small businesses have fewer resources and pose less of a risk to data protection, so there may be more leniency by the ICO in relation to any non-compliance.
- Even if your company falls under one of the exemptions, if you're contracting with a larger company that conducts large-scale processing you may also be subject to the harsher end of the GDPR's regulation.

Rutland County Council

9. Prepare to comply with access rights

- Prepare to meet access requests within a one-month timeframe.
- **Subject Access Rights**-citizens have the right to access all of their personal data
- **Rectification**- rectify anything that's inaccurate
- **Objection**- object to processing in certain circumstances
- **Erasure**- completely erase all of their personal data that you may hold.

Rutland County Council

Things that you may need to do?

Keep Records

Small businesses only have to keep records if data processing is:

- Regular
- A threat to people's rights and freedoms
- Dealing with sensitive data or criminal records

Records should contain:

- Name and contact details of business
- Reasons for data processing
- Description of categories of data subjects and personal data
- Categories of organisations receiving the data
- Transfer of data to another country or organisation
- Time limit for removal of data, if possible
- Description of security measures used when processing, if possible

Rutland County Council

Anticipate With Impact Assessments

Impact assessments may be required for HIGH-RISK processing, for example:

- New technologies
- Automatic, systematic processing and evaluation of personal information
- Large-scale monitoring of a publicly accessible area (e.g. CCTV)
- Large-scale processing of sensitive data like biometrics

Rutland County Council

What are the GDPR penalties?

- Businesses in breach will see a dramatic increase in fines with **penalties reaching an upper limit of €20 million or four per cent of annual global turnover, whichever is higher**.

- Insolvency will be a real risk for non-compliant businesses as a result of these fines. But bear in mind the possibility that individuals can also sue you, if they suffer as a result of your data management. This could be for material damage or non-material suffering, such as distress

Rutland
County Council

QUESTIONS?