The General Data Protection Regulation (GDPR) factsheet

For Intermediary Use Only

SKIPTON INTERMEDIARIES

What is GDPR?

On 25 May 2018 the General Data Protection Regulation (GDPR) will replace the UK Data Protection Act 1998 (DPA).

The GDPR will update existing data protection law by strengthening people's rights, increasing compliance obligations and expanding regulator enforcement powers. GDPR will also impact how organisations process personal data and the controls and governance around those activities.

This factsheet provides information about the new regulation, our plans at Skipton and the changes you might want to consider in the coming months.

What is personal data?

The following are examples of different categories of personal data.

Personal details

- Title, name, address, date of birth, age, national insurance number, gender, passport number, appearance
- Contact details, email address and phone number
- Family details, dependents, next of kin, power of attorney.

Product and services

- Customer information - products and services purchased, customer ID, annual general meeting membership, online/offline customer, marketing preferences
- Customer Interactions - system notes, emails about customers, customer complaints, letters to and from customers, notes from reviews and call recording.

Education and employment

- Employment history, applications, holiday/absence records, salary, job title, disciplinary actions, performance reviews, colleague number, pay as you earn code
- Education, schools attended, qualifications.

This fact sheet aims to provide an overview of GDPR and does not set out all the requirements which firms may need to comply.

What's changing at Skipton?

- We'll be reviewing our marketing consent wording to ensure it meets the new standard and making our marketing consent questions more prominent. We'll also be giving customers explicit 'yes' and 'no' options when we ask for their consent.
- We'll be reviewing our privacy notices, for example, in our mortgage application forms and website, to ensure they're transparent and include all the required information.
- We'll be updating our breach notification policy to make sure we're able to notify the Information Commissioner's Office (ICO) within 72 hours if there is a data security breach.
- We'll be reviewing our contracts with suppliers and undertaking revised due diligence to ensure they meet the new GDPR standard and have appropriate processes and controls in place to handle customer data.
- We'll be introducing data protection impact assessments to assess and manage data protection risks.
- We'll be updating our internal records of processing to ensure we know what data we hold and why.
- We'll be reviewing and updating our processes for handling individual rights, including new rights such as the right to erasure (alternatively known as the right to be forgotten).

How will this affect me?

All organisations that process personal data are likely to be affected by the introduction of GDPR. Here are the key changes.

- **Transparency** - whereas the DPA provided a good deal of discretion, GDPR is a lot more specific about what information must be provided to people about how their personal data is processed.
- **Accountability** - GDPR requires organisations to demonstrate compliance. This includes things like maintaining up to date policies and procedures.
- **Consent** - the standard for obtaining valid consent is much higher with GDPR, so consent should only be used when absolutely necessary.
- **New and strengthened rights** - in the majority of cases it will no longer be possible to charge a fee for dealing with a customer data request, and the time limit for responding to requests will be reduced to one month. Other new and strengthened rights under GDPR include:
  - The right to erasure – a person has the right to ask for their personal data to be deleted if it's no longer necessary for it to be kept. See the FAQs for more detail
  - The right to object – a person has the right to object to certain types of data processing based on their particular circumstances
  - The right to data portability – a person has a right to obtain a copy of the information they have provided in a commonly used, machine-readable format (such as a CSV file) and to transfer it to another organisation.
- **Personal data breaches** - these must be reported to the Information Commissioner's Office (ICO) within 72 hours where there's a risk to an individual. Where there is a high risk, impacted individuals must also be notified.
- **Record of processing activities** – records must be kept by certain organisations and detail the why, who, what, when and where about processing activities.
- **Data processors** – people who process data on behalf of a controller have direct obligations under GDPR. Contracts with processors should be reviewed to ensure they are GDPR compliant, the ICO's Guide to GDPR that's available on their website provides helpful guidance on what to include.

FAQs

Q. What is the new standard for consent?

A. Requests for consent will have to be clearly distinguishable under GDPR, for example, they shouldn't be 'hidden' in terms and conditions. Pre-ticked opt-in boxes will also be invalid. Organisations will also need to consider how to demonstrate they have a person's consent, for example, by recording when consent was given and what it was given for. Organisations will also have to consider updating any current consent that doesn't meet the new standard if they plan to continue relying on consent under GDPR. It's worth bearing in mind that consent is not the only way of lawfully processing a person's data.

Q. Does Brexit mean the GDPR won't apply to the UK?

A. No – GDPR will come into force in the UK on 25 May 2018 and will not be affected by Brexit, even after we've left the EU.

Q. When does the right to erasure apply?

A. If a person exercises their right to erasure (right to be forgotten) it doesn't automatically mean all their data has to be deleted. Restrictions mean data will only need to be deleted in certain circumstances, for example, if it's no longer necessary for a firm to hold that data. The right does not apply to personal data that's required for the defence of legal claims. A record retention schedule setting out how long you require different types of personal data and when it should be deleted, could be helpful when responding to a right to erasure request.

Q. What is the lawful process to capture data?

A. The lawful bases for processing data under GDPR are in essence similar to those under the DPA. It is suggested firms identify and document the legal basis for each of their processing activities and communicate these in their Privacy Notice.

Next Steps

1 The data you hold
have you considered?

- what data you currently hold
- how you capture data
- where it's saved
- where it came from
- how you share it
- how long do you keep it for

2 Marketing consent

What changes do you need to make to how you capture data and record consent?

3 Data breaches

What's your plan to deal with data breaches?

4 Data requests

What process will you follow when you receive requests?

Call **0345 266 0973**
8am - 8pm Monday to Thursday,
8am - 5.30pm Friday, 9am - 12pm Saturday

Email **irmsupport@skipton.co.uk**
Visit **skipton-intermediaries.co.uk**