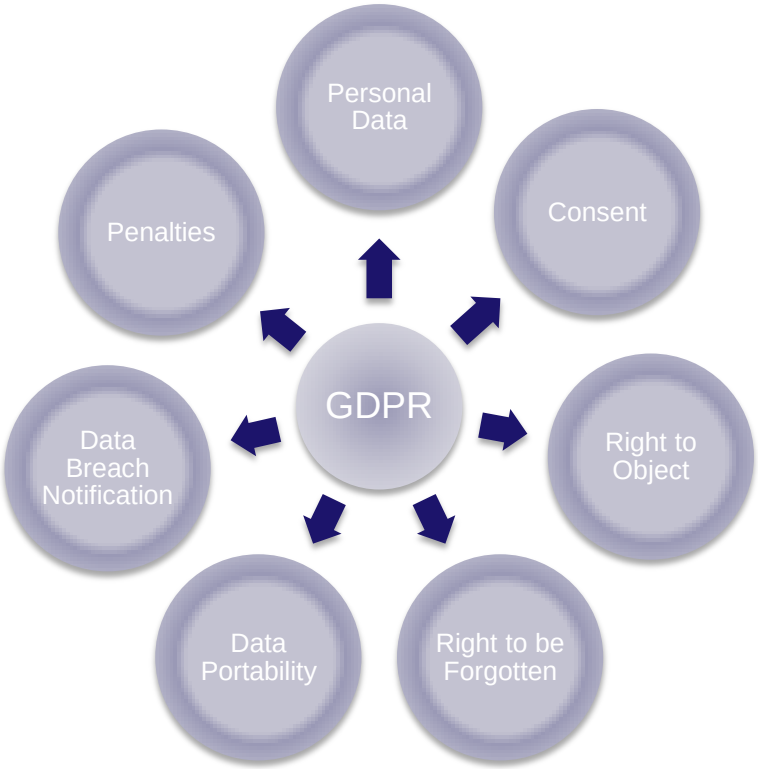
eazipay®
We make your cashFLOW

A guide to GDPR – the effect on all UK organisations



A white paper from Eazipay Ltd
October 2017

Introduction

Eazipay is one of the UK's leading automated payment processing companies. We currently provide regular Direct Debit and other automated payment services to over 1,600 SMEs and corporate organisations in a wide range of market sectors throughout the UK, Europe and beyond.

With more than 20 years' experience we are perfectly placed to help businesses improve cash-flow and save time and money by establishing regular automated payment collections.

This guide has been created to provide an overview of the General Data Protection Regulation (GDPR) and its ongoing impact to all businesses from its implementation date of 25th May 2018.

Before then all EU based organisations that store and process the personal data of EU residents have only a short time to ensure they are compliant.

Use the data in this guide to stay ahead of the regulation and realign corporate procedures to meet the new regulatory requirements.

Contents

GDPR and its application

The EU General Data Protection Regulation (GDPR) will come into effect in the UK and EU-wide from 25th May 2018 and will affect everyone involved in collecting and processing data about individuals in the context of selling goods and services.

The aim of GDPR is to protect all EU citizens from privacy and data breaches in an increasingly data-driven world that is vastly different from the time in which the 1995 Data Protection Directrive was established.

GDPR was designed to harmonise data privacy laws across Europe, to protect and empower EU citizens' data privacy and to reshape the way organisations approach data privacy.

If your business undertakes the control, collection of data from EU residents, or processes data on behalf of a data controller (inlcuding cloud based service providers, call centre and payroll services), then it is likely that you will be subject to the GDPR.

GDPR introduces a new accountability requirement that expects organisations to show how they comply with the principles – for example, by documenting the decisions taken about a processing activity.

Key points

The GDPR places greater emphasis on the documentation that data controllers must keep to demonstrate their accountability. Compliance with all the areas of the regulation will require organisations to review their approach to governance and how they manage data protection as a corporate issue. One aspect of this might be to review the contracts and other arrangements in place when sharing data with other organisations.

Opt-in replaces Opt-out.

The 'opt-out' option is a familiar part of marketing communication these days.

"If you don't want to hear from us again, tick this box or click this link".

Under GDPR the Opt-out option will be no more. Instead, **Opt-in** consent will be required for all marketing communications.

Requests for **personal information** can be made free-of-charge by individuals. When someone asks a business for their data, they must provide the information within one month.

The **right to be forgotten** is strengthened. Individuals now have the right to force data controllers to delete all information they hold on them, including any details retained on a "do not contact" list. Businesses will have to work out new processes to ensure all personal information is thoroughly and permanently erased.

The right to **rectify inaccurate personal data** is also afffected. Under the new rules individuals can request that personal data is supplied in a transferable and viewable file, and all requests must be adhered to.

The right **not to be subject to a decision** based solely on automated processing of data is also affected, where requested organisations must provide individuals with an explanation of a decision made about them.

The GDPR also requires data controllers to conduct a **Privacy Impact Assessment (PIA)** where privacy breach risks are high to minimise risks to data subjects in advance to handling personal information.

Business systems are to be designed and used with privacy of personal data as a prioitiy. Data controllers and processors will have to hold and process only the data absolutely necessary for the completion of its duties, as well as limiting the access to personal data to only those idividuals within the organsiation needing to act out the processing.

Global suppliers will also have to adhere to GDPR when handling data for a EU based organisation.

What is personal data?

Personal data means any information relating to an identified or identifiable natural person ('data subject').

The scope of personal data has been extended to include online identities, incorporating:

- full name
- job title
- work email address
- personal email address
- phone numbers
- home address
- online identities
- cookies
- IP address
- health records
- biometric data
- genetic data

Do you need a Data Protection Officer?

The **Information Commissioner's Office** will continue to enforce these data laws.

Organisations must appoint a Data Protection Officer (DPO) in the case of: public authorities, organisations that engage in large scale systematic monitoring, or organisations that engage in large scale processing of sensitive personal data.

If your organisation doesn't fall into one of these categories, then you **do not** need to appoint a DPO.

Evidence of company compliance must be recorded within organisational procedures, and for larger companies with more than 250 employees there is a requirment to document why personal information is being collected and processed; details of the information held; how long it's being kept for and descriptions of technical security measures in place.

This also includes automated data functions.

Breaches

GDPR continues to oblige UK based organisations to report data breaches to the Information Commissioner's Office.

The notice must be made within **72 hours** of data controllers becoming aware of it, with the exception of only extraordinary circumstances that will require justification.

Where the risk to the individual is high, - such as financial implication, the risk of personal rights being affected or loss of reputation - the subject must be personally notified.

Systematic supply chain reviews and audits will be required under the GDPR rules to ensure they are compliant. Regular periodic data protection audits can be enforced following a written warning of first cases and non-intentional non-compliance.

Penalties

The Information Commisioner's Office could enforce much higher fines than those currently in place - up to 4% of annual global turnover for breaching GDPR or €20 million, whichever is greater.

This is the maximum fine that can be imposed for the most serious infringements, e.g. **not having sufficient customer consent to process data** or **violating the core of Privacy by Design concepts**.

There is a tiered approach to fines, e.g. a company can be fined 2% for not having their records in order, not notifying the supervising authority and data subject about a breach, or not conducting impact assessments.

All of these rules apply to both data controllers and data processors.

Take action now

It's imperative that UK businesses act now to ensure compliance before May 2018, to train staff and to update data processing procedures.

Review your practices to establish whether your current level of **'Opt-in'** meets the new terms. Amend your **consent terms**, contact every person you wish to communicate with in the future to upgrade their consent level to the new standard and start storing consent forms.

Review all **data protection policies**, data protection impact assessments and ensure you document how data is processed.

Implement the plan now; being ahead of the game could provide a huge competitive advantage.

About Eazipay

Eazipay helps businesses large and small access the power of automated payment services such as Direct Debit.

Our success is down to our attention to detail and the level of service we provide. Every customer, no matter what their size, receives the same high quality of care. We know that integrating automated payments like Direct Debit into your accounts system will have real, tangible, measurable benefits for your business.

Eazipay has been awarded 'Affiliate' status from Bacs, the governing body for Direct Debit in the UK. We are now a member of an exclusive group of 55 other Bacs Affiliates, which includes representatives from some of the UKs leading businesses, banks and building societies, as well as government organisations and banking technology providers.

We are also recognised as a Bacs Approved Bureau, which demonstrates that our operational processes and expertise not only meet, but exceed, exacting industry standards.

As well as our Bacs Approved and Affiliate stats, Eazipay was one of the first Direct Debit bureaux to receive ISO9001:2015 certification for Quality Management System and direct authorisation from City watchdog, the Financial Conduct Authority (FCA).

We are working ahead of the regulation implementation to ensure that personal data is stored within our internal system and this adheres to the GDPR rules. We will be in touch with all our existing clients to request consent to hold their data, and to ensure that they are conforming to the new rules with regards to their customers' data.

Further reading

Details in this guide were sourced from the following resources:

- Information Commisioner's Office
- IT Governance
- UK Parliament Data Protection Bill (HL Bill 66)
- REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Useful further reading

- The Information Commissioner's Office has issued a 12 step guide

Call us on: 01353 864 949
Email us on: sales@eazipay.com
Or, you can write to us or find us here:
Sydney House
Unit 62
Lancaster Way
Ely, Cambridgeshire
CB6 3NW