Becoming GDPR compliant

A beginner's guide

Simply Mail Solutions

simplymailsolutions.com

Introduction

At Simply Mail Solutions (SMS) we've been helping organisations use cloud services to improve their communications, productivity, and processes for over 10 years. Over 4,000 customers trust us to support their online business activities through powerful tools and first-class UK support.

We know the forthcoming General Data Protection Act is a growing concern for our customers, as well as the wider business community and we've put together this simple guide to what the GDPR is, and how to check you'll be compliant. Being a cloud-based company we've also included details of some modern business productivity tools that help.

Disclaimer

Whilst every attempt has been made to ensure accuracy, SMS makes no warranties, express, implied, or statutory, as to the information in this white paper. Information is supplied 'as-is' and you must not rely on this white paper as an alternative to legal advice from a lawyer, or regulatory body.

What is the GDPR?

The GDPR ('General Data Protection Regulation') is the European Union's replacement for the Data Protection Directive (which was implemented in the UK under the Data Protection Act 1998). It takes effect from 25 May, 2018 and **all businesses which collect, or process, personal data of EU residents must comply with the regulations from this date.**

What are the main requirements of the GDPR?

The GDPR defines a wide range of requirements that organisations collecting, or processing, personal data must follow. The requirements are based on six key principals:

- Transparency, fairness, and lawfulness — Organisations must be clear with individuals how personal data is used and there must be a 'lawful basis' for processing it
- Limiting processing of data — Any processing must be for specified, explicit, and legitimate purposes. You cannot reuse or disclose personal data for purposes which are not compatible with the original purpose it was collected for
- Minimising the collection and storage of personal data — Data should only be collected and stored for specific and relevant reasons
- Ensuring accuracy of personal data and enable it to be erased or rectified — Organisations need to take steps to make sure personal data is accurate and can be corrected if errors occur

- Limiting the storage of personal data — Personal data should only be stored for as long as necessary to achieve the purposes for which it was collected
- Ensuring security, integrity, and confidentiality — Organisations must take steps to keep personal data secure by technical and organisational security measures

What are a person's rights under the GDPR?

The GDPR gives individuals certain rights, these are:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- The right not to be subject to automated decision-making, including profiling

These rights build on, and enhance, rights already provided in law. The right to data portability is new and applies to:

- Personal data an individual has provided to a controller;
- where the processing is based on an individual's consent or for the performance of a contract;
- and when processing is carried out by automated means.

Portable data needs to be provided in a commonly used and machine readable form, and without charge.

Who does the GDPR affect?

The GDPR affects all organisations, of any size and industry sector. If an organisation processes any personal data for an EU citizen, regardless of where the processing takes place, then the GDPR applies to how the data is handled.

The data protection regulators in many EU states have already said there will be no grace period for organisations which are non-compliant after 25 May, 2018.

How does the GDPR define 'personal data'?

The GDPR takes a broad definition of personal data and classifies it as any data that relates to an identified or identifiable natural person.

Personal data includes, but is not limited to:

- Online identifiers such as IP addresses
- Employee information
- Sales databases
- Customer services databases
- Customer feedback forms
- Location data
- Biometric data
- CCTV footage
- Loyalty scheme records
- Health information
- Financial information
- Pseudonymized data, where the pseudonym can be linked to an individual

The definition is much broader than you may think. For example, a photograph with no people in it (eg a photograph of an empty beach) can still be classed as personal data if it is linked by a unique code to an individual (such as an online photo storage service using the filename to link to a person's account).

How can you be compliant with the GDPR?

Every organisation needs to prepare for the GDPR and planning should start now. Leaving it till May 2018 will be too late, especially where changes to processes or business tools are needed. Here are the key checklist points identified by the Information Commissioner's Office (ICO).

Raise awareness

Understand who the key stakeholders are in your organisation and make them aware of their GDPR requirements. Implementing the GDPR is likely to impact on business resources and take time, so have stakeholders take responsibility for their own section's responsibilities.

Document current information

The GDPR requires you to maintain records of your data processing activities, and how data is used and shared. For example, if you hold inaccurate data on an individual and have shared this data with another organisation then it is your responsibility to inform the other party and ask them to update their records.

Unless an organisation understands what data is held, and how it is processed and shared, you won't be able to comply with the GDPR. This means a complete audit of personal information is required. This will help stakeholders understand their requirements, demonstrate compliance, and develop effective processes for handling data once the GDPR become active.

Communicate privacy information

Is your organisation's current privacy notice accurate? When collecting personal data you have to give people details on your identity and how you intend to use their information. Under the GDPR there are additional things you must tell people, such as the lawful basis for you to process data, your data retention periods, and an individual's rights to complain to the ICO.

This information must be relayed in concise, easy to follow, clear language. Planning for the GDPR is the time to study your existing privacy notices and update them.

Understand an individual's rights

We've already covered the basics of what an individual's rights are under the GDPR, make sure your organisation understands the details of those rights; answering questions now not after things change.

Update access request procedures

The GDPR updates how a company must respond to data access requests:

- In most cases organisations can't charge for access to data
- The time limit for responding drops to a month
- You can refuse a request that are manifestly unfounded or excessive
- You must inform the individual of any refusals, giving reasons why and inform them they have the right to complain to the supervisory authority and to a judicial remedy. A person must be informed of the refusal promptly; at the latest within a month

Large organisations which may potentially receive a large number of requests may need to revise procedures to make sure that the new, tighter, timescales can be met.

Identify lawful basis for processing personal data

Under the GDPR some individual's rights will be modified based on the lawful basis for processing personal data. For example, if you are using consent as the lawful basis then the person has a stronger right to to have their data deleted.

Organisations need to fully understand the lawful basis for processing data and explain the basis in your privacy notice. Documenting the lawful basis will help with 'accountability' compliance.

Review how consent is managed

Reviewing how an individual consents to having their data processed will help organisations ensure they meet the DGDPR's requirements. Consent must be:

- Freely given
- Specific

- Informed
- Unambiguous

Opt-ins must be positive (not 'tick this box to confirm you don't want to receive marketing information') and consent cannot be inferred from pre-ticked boxes or 'silence'.

Understanding consent is a big area of the GDPR and the ICO have published detailed guidelines to help organisations understand the requirements. You can download the pdf here:

https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf

Review processes for handling children's data

For organisations which process children's information, there are new requirements for obtaining consent and special protections to consider.

An organisation offering online services to minors, which relies on consent to collect information, may require the consent of a parent or guardian to process data lawfully. The GDPR sets the minimum age a child can give their own consent as 16 (this may be lowered to 13 in the UK - Check with your legal advice to confirm before the May 2018).

For services aimed at children, the privacy notice must be written in language a child will understand. Organisations may need to rewrite their privacy policies to comply.

Reporting and investigation data breaches

The GDPR creates a duty on all organisations to notify the ICO, and in some cases individuals, when a breach is likely to result in a risk to a person's rights and freedoms, for example:

- Discrimination
- Loss of reputation
- Financial loss
- Loss of confidentiality
- Significant social or economic disadvantage

Organisations should re-assess their current processes for detecting, reporting, and investigating data breaches.

Mandating Data Protection by Design and Data Protection Impact Assessments

The GDPR makes privacy by design a legal requirement and Data Protection Impact Assessments (DPIA) are also mandatory in certain situations.

DPIA's are required where data processing is likely to lead to a high risk for individuals:

- Where new technology is being deployed
- Where a profiling operation is likely to significantly affect a person
- Where there is large scale processing of the special categories of data

If a DPIA highlights an area where data processing is high risk, and it is not possible to sufficiently address them, you are required to consult the ICO and seek its opinion.

Designate a Data Protection Officer

Some organisations will need to formally designate a Data Protection Officer (DPO):

- A public authority (except for courts acting in their judicial capacity)
- Organisations carrying out large scale regular and systematic monitoring of individuals
- Organisations carrying out large scale processing of special categories of data, like health records or criminal convictions.

If your organisation does not need to formally designate a DPO it is still recommended as best practice, given the increased requirements of the GDPR

Establish a lead authority for pan-EU operations

Organisations operating in more than one EU member state should determine a lead data protection supervisory authority and document it.

The lead authority is the supervisory authority in the state where your main establishment is. This is either:

- The location of your central administration in the EU; or
- The location where decisions about the purposes and means of processing data are taken and implemented

Cloud business tools to help compliance

Hopefully it is now clear what changes your business needs to make to meet the new GDPR requirements. Adapting to the new rules, and maintaining compliance in the future, may seem a Herculean task; however modern cloud-based business tools can help ease the transition to the new framework.

Azure

The Microsoft Azure Data Catalog keeps a record of data sources used by your organisation. Registering a data source in the Data Catalogue keeps its meta data indexed making it easier to search and discover the data in the future.

The Azure Security Center provides visibility and control over Azure resources. It offers security recommendations and helps prevent, detect, and resolve threats.

Data encryption secures data at rest (on the server) and in transit, preventing unauthorised people from obtaining usable data.

Dynamics 365

Role-based security means individuals only have access to certain data, or can perform limited tasks, reducing the risk of an employee obtaining information they shouldn't.

Record-based security restricts access to specific records, locking unauthorised employees out.

The Report Wizard tool simplifies the extraction of information to ensure compliance, for example identifying individuals who have not opted-in to data collection.

Microsoft Intune

Devices can be encrypted, information selectively wiped, and controls placed on which applications store data.

Microsoft Office 365

Data Loss Prevention identifies over 80 common sensitive file types, including financial and medical information, and allows organisations to configure actions to be taken upon identification.

Advanced Data Governance uses machine learning to find, classify, and set policies for, the most important data in your organisation.

eDiscovery uses advanced searching techniques to find text and meta data across all the organisations Office 365 assets. Useful for finding all information relating to an individual.

Advanced Threat Protection in Office 365 email protects against email attacks which could otherwise lead to data loss.

Office 365 audit logs monitor and track user activities across workloads, helping with early detection of potential compliance issues.

Conclusion

The GDPR makes many new demands on organisations, and tightens existing restrictions. With the authorities stating no grace period beyond May 2018 it's essential to begin planning implementation now. The topics raised in this white paper will help you understand your requirements under the GPDR and assist you in the planning stage.

There are cloud business tools which simplify many of the implementation and on-going compliance needs, and organisations are recommended to utilise them.

Further information

For information on what cloud business tools are available, contact SMS on +44(0)1925 818448, sales@simplymailsolutions.com or visit our website: simplymailsolutions.com

The ICO maintain a wealth of information on the GDPR and how to comply. The best place to start is the overview page on their website: https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/

Microsoft's GPDR microsite, has more information on how their technologies can help: www.microsoft.com/gdpr

Checklist

Use this checklist to make sure you've followed all the recommended steps on the journey to GDPR compliance.

Completed?	Topic
	Raise awareness
	Document current information
	Communicate privacy information
	Understand an individual's rights
	Update access request procedures
	Identify lawful basis for processing personal data
	Review how consent is managed
	Review processes for handling children's data
	Reporting and investigation data breaches
	Mandating Data Protection by Design and Data Protection Impact Assessments
	Designate a Data Protection Officer
	Establish a lead authority for pan-EU operations

Microsoft Office 365

Office 365 provides many built-in tools to help businesses manage compliance. These tools work across Office 365's range of integrated services.

What's included	How it helps compliance
Data Loss Prevention (DLP)	Identifies more than 80 common sensitive data types including financial, medical, and personally identifiable information. Organisations can configure actions to take when sensitive data is identified and prevent accidental disclosure. **GDPR places special requirements on businesses to manage identifiable information — especially sensitive data.**
Advanced Data Governence	Finds and classifies the data most important to your business through machine-assisted intelligence and insights. Once found policies can be set to control the data's usage. **GDPR complies businesses to manage how they process data, and only store it for as long as is required.**
Office 365 eDiscovery	Searches through text, and metadata, across Office 365 service to easily find required information. Office 365 E5 plans go further with Advanced eDiscovery through machine-learning to eliminate duplicate results, and identify themes and relationships. **GDPR requires businesses to quickly identify a customer's data and delete records when requested.**
Customer Lockbox	Requirers customer approval for Microsoft engineers to access data stored on your account when completing service requests. **GDPR complies businesses to manage how third-parties access their data.**
Exchange Online Advanced Threat Detection (Optional service)	Protects emails against new, sophisticated malware in real-time. Allows businesses to create policies to prevent users accessing dangerous attachments and websites. Threat intelligence proactively uncovers threats through the Intelligent Security Graph. **GDPR requires business to protect data against online theft, and other threats.**
Advanced Security Management	Identifies high-risk and unusual behaviour by employees accessing Office 365 services, alerting businesses to potential security breaches. **GDPR requires business to protect data against online theft, and other threats.**
Audit logs	Monitors and tracks user or administrator activities across Office 365 services, assisting early detection of compliance dangers. **GDPR requires business to protect data against online theft, and other threats.**

SMS
Your Partner In The Cloud

Contact SMS on +44 (0) 1925 818448 or sales@simplymailsolutions.com

Microsoft Enterprise Mobility + Security

Securing personal data across devices and platforms, both in the cloud and on-premises is a core part of being GDPR compliant. EM + S makes it easier for IT departments to control data access and maintain flexible working patterns.

What's included	How it helps compliance
Multi-Factor Authentication	Sets policies, and manages, employee account access to safeguard company data by enforcing authentication via multiple methods (password and an authentication app for example). **GDPR compels businesses to control access to data.**
Microsoft Cloud App Security (Included with EM + S E5, available as an add-on for EM + S E3)	Identifies cloud apps used by employees and assigns a risk score to each service. Give businesses the power to control usage of cloud apps. **GDPR requires businesses to manage third-party access and storage of customer data.**
Remote device wiping	Quickly wipe a remote mobile device (iOS, Android, or Windows) or selectively wipe business information and leave the owner's personal data intact. **GDPR requires businesses to secure an individual's data.**
Intune App Management	Assign specific apps to to specific users and devices. Protect company data within apps and remotely wipe information if required. **GDPR compels businesses to control access to data.**
Azure Information Protection	Classifies data based on sensitivity, encrypts data with defined usage rights and protects data within and outside your corporate infrastructure **GDPR compels businesses to control access to data and manage third-party access to information.**
Microsoft Advanced Threat Analytics	Pinpoints business breaches and identifies attackers through advanced behavioural analytics and detection technology. Reduces time to identify and report attacks, speeding up response and minimising danger. **GDPR requires businesses to secure an individual's data.**

SMS
Your Partner In The Cloud

Contact SMS on +44 (0) 1925 818448 or sales@simplymailsolutions.com

The SMS advantage

Microsoft Office 365 delivers a wealth of tools to help achieve GDPR compliance. SMS add an extra layer of support and services to make compliance easier.

SMS advantage	How it helps compliance
24 x 7 x 365 Support	Whenever support is needed, SMS is there. Our skilled UK-based team can help you resolve issues promptly and keep your services running smoothly. **GDPR complies businesses to control and secure data. World-class support aids this.**
ISO Certification	With both ISO9001:2015 and ISO27001:2013 certification SMS demonstrate their commitment to the highest levels of customer focus and data security. **GDPR complies businesses to ensure third-parties processing or hosting data meet the highest standards.**
On-going account management	SMS keep you informed on services which benefit your business operations and processes, highlighting ways to use cloud technology and keep to best-practice. **GDPR requirements will change over time, SMS keep you updated on the latest details and how to stay compliant.**

SMS are here to support your GDPR journey and help you maintain compliance. Please contact us with any questions you have over how cloud services aid your business aid and processes.

Email: sales@simplymailsolutions.com
Tel: +44 (0) 1925 818448 (UK business hours)