GDPR 2018 Compliance Requirements

Latest Revision: 22nd February 2018

What Is GDPR and When Will It Come into Effect?

New General Data Protection Regulation (GDPR) will come into effect on 25th May 2018 replacing the 1998 UK Data Protection Act. The purpose is essentially to expand the rights of individuals and how their data is collected and processed, ultimately returning control to citizens over the use of their data. Organisations will be held more accountable for data protection – how they hold and process consumer data. Consumers will also be given enhanced privacy protections, including the right to access data held about them and to have it permanently deleted upon request. Organisations will also be required to inform the Information Commissioner's Office (ICO) of any data breaches.

Terminology – What Is Personal Data?

In principal, personal data refers to any information which relates to an identifiable, living human being and typically includes the following:

- Name
- Address
- Email address
- Photo
- IP address
- Location data
- Online behaviour (cookies)
- Profiling & analytics data
- Race
- Religion
- Political opinions
- Trade union membership
- Sexual orientation
- Health information
- Biometric data
- Genetic data

Organisations will need to establish if they are legally allowed to collect, hold or process data, where it is held and for what purposes.

Terminology – What Is the Difference Between a Data Controller, Data Processor and a Data Subject?

A **Data Controller** is an entity which determines the means, conditions and purposes of the processing of personal data – in short, how the data is or will be used. The **Data Processor** is the entity which processes personal data on behalf of the controller – processing is obtaining, holding, recording or adapting personal data.

The **Data Subject** is a living individual whom the particular personal data is about.

Who Does GDPR Apply To?

GDPR applies to all UK organisations including public authorities, commercial businesses and charity organisations. It aims to introduce stronger consent requirements making organisations more accountable for data protection, i.e. how they hold and process consumer data. It also applies to all companies holding and processing personal data of Data Subjects residing in the EU, regardless of the company's physical location.

GDPR and Brexit

The UK government has stated that it will comply with GDPR when it comes into effect on May 25th 2018 – compliance will not be affected by Brexit as GDPR will be assumed into UK law before exiting Europe.

What Are the Key Changes of GDPR?

Consent

GDPR introduces stronger consent requirements, giving the Data Subject improved control over how their data is used. Organisations will need to show how and when consent was given – passive consent will no longer be acceptable (pre-ticked boxes or opt-out boxes will not qualify as consent).

Businesses will need to create a framework in which privacy is at the forefront of processes and procedures. Safeguards must be in place to ensure all data is stored accurately and confidentially. In the case of data being supplied by an external company, organisations should ensure third parties are themselves compliant.

The request for consent must be presented in a readily accessible, and easy to understand manner. This should be clearly displayed and easily recognisable and should not contain legal terminology or technical jargon which may be confusing or illegible to the average reader.

The Data Subject must be able to easily withdraw consent if necessary. The form should include, for example, a checkbox with text clearly stating that it requires the consent of the Data Subject to store and use their data. This checkbox will be unchecked as default and provide an 'opt-in' request to the Data Subject that needs explicit action from them to agree and to be able to continue.
It may not be presented as a pre-checked 'opt-out' request, which requires the Data Subject to uncheck the box to signal their non-compliance.

The Right to Be Forgotten/Data Erasure

Data Subjects are entitled to request the Data Controller to erase or forget their personal data and cease from further dissemination (this may also include third parties).

Conditions under which the Data Subject may make a request for erasure include, the withdrawal of consent or data no longer being relevant to the original processing.

Note: in some situations, the Data Controller will be required to evaluate the Data Subject's rights in relation to the public interest of availability of information.

Data Portability

The Data Subject has the right to receive personal data concerning themselves, as well as the right to transmit this data to another controller.

Penalties

The maximum fine imposed for the most serious infringements of GDPR breach, such as not having consent to process data, is up to 4% of annual global turnover – or a fine of €20 million, whichever is greater. Penalties will be tackled with a tiered approach depending on the severity of the breach.

Access to Data

Data Subjects have the right to confirmation from the Data Controller as to whether or not data regarding themselves is being held or processed, and if so, for what purposes. Currently organisations (including public bodies) are able to charge £10 for a Subject Access Request (SAR). GDPR is removing this fee and requests for a copy of personal information are to be made available in electronic format, free of charge.

Data Protection Officers

Under GDPR some organisations are required to appoint a Data Protection Officer (DPO), specific provisions are laid out in GDPR with regards to the tasks a DPO should carry out.

A DPO must be appointed under GDPR for the following:

- public authorities
- organisations which carry out large scale systemic monitoring of individuals
- organisations which carry out large scale processing of special categories of data, or data relating to criminal convictions and offences

Not all organisations are obliged to appoint a DPO, they must however, ensure they have adequate staff and skills to discharge their obligations under GDPR; this includes advising the organisation and its employees on their obligations to comply with GDPR, monitoring compliance and acting as a point of contact for supervisory authorities and Data Subjects.

Breach of Data

Following a breach of data, GDPR states that the ICO must be informed of the breach within 72 hours of first becoming aware of it. Any Data Processors must also notify Data Controllers and subjects impacted by the breach.

Data Protection by Design

The inclusion of data protection is to be integrated into the initial design of an organisation's website by default, rather than in addition at a later date. This in many cases will require investment into data protection controls and processes.

Pseudonymisation – the Separation of Data from Direct Identifiers

The term 'Pseudonymisation' is referred to in GDPR – essentially a safe guarding mechanism against being able to personally identify information, this is one of the core pillars of GDPR. Pseudonymisation introduces a new concept of processing data which means it is neither anonymous, nor directly identifiable. This processing system, in its most basic form, uses a unique reference ID for an individual rather than their actual name when storing on a database. The Data Subject's personally identifiable information would be then stored on a separate database, the data could only be recreated by joining the tables together. In the event of a breach of data, no names would be exposed – merely the reference ID.

Age of Consent

GDPR contains new regulations intended to improve the protection of children's personal data. A child is defined as an individual below the age of 16, any services offered directly to a child will require a privacy notice written in a clear manner which will be easily understood by a child.

A child under the age of 16 cannot give consent to process their own data, consent is required from a person holding parental responsibility. For websites offering an online service to children, permission from the child's guardian may be required in order to process data.

Third Party Data Processors

Systems such as Mailchimp, Campaign Monitor, Google etc. are considered Third Party Data Processors, meaning they process data on behalf of the Data Controller. Most large US based Data Processors such as Google are currently in the process of becoming fully GDPR compliant and many of which have already done so. It remains however, the responsibility of each organisation to ensure that any Third Party Data Processors used, are fully compliant. This information can usually be located in the privacy policy of the Third Party.

Making Your Website GDPR Compliant

Data Collection and Processing

Identify all of your Data Processors, which of these are Third Party and if Third Party processors are GDPR compliant.

Having identified all Data Processors, the next step is to establish if you have satisfied the following regulations for storing data:

- Are you legally allowed to collect this data?
- Are the Data Subjects fully aware of what data is being collected and for what purposes?
- What is the source of the data?
- What are the categories of Data Subjects?
- Does the nature of the data being collected fall into what is defined by GDPR as a special category of personal data?
- Have the Data Subjects been clearly notified of their rights?
- Where is the data being stored?
- Is the data transferred to a country outside of the EU? If so, to which country is it transferred?
- Do you need to keep the data? If so, for how long?
- What is your organisation's method of destruction of data after it has passed its retention date?

Consent

Ensure your organisation satisfies the high GDRP regulations regarding consent by addressing the following points taken from the ICO:

- Ensure that consent is the most appropriate lawful basis for processing
- The request for consent should be prominent and separate from your terms and conditions and privacy policy
- Consent requires a positive opt in
- Do not use pre-ticked boxes, or any other type of consent by default
- Always use clear, plain language that is easy to understand
- Specify why your organisation wants the data and what they intend to do with it
- Use specific granular options to get separate consent for independent processing operations
- Name any Third Party organisations which may rely on the consent
- The process of withdrawal of consent must be straightforward, easily accessible and transparent
- An individual must be able to refuse to consent without detriment

- Consent should not be a precondition of a service
- When offering online services directly to children, only seek consent if there are age-verification and parental-consent measures in place

Recording Consent

- Ensure a record is kept of when and how consent was given from the individual
- Keep a record of exactly what Data Subjects were told at the time

Managing Consent

- Consent should be reviewed on a regular basis to check that the relationship, processing and the purposes have not changed
- There should be processes in place to refresh consent at appropriate intervals, such as any parental consents
- The use of privacy dashboards or other preference management tools are considered a matter of good practice
- Withdrawal of consent for individuals must be easy and how to do so, well publicised
- Requests for withdrawals of consent must be acted on as soon as possible
- Individuals who wish to withdraw consent must not be penalised

Data Protection Officer

- Establish if your organisation requires a Data Protection Officer
- If this role can be provided by an existing member of staff, the role must be fulfilled without interference from the demands of their existing role or by other members of staff

Breach of Data

- A breach of data must be reported to the ICO within 72 hours of becoming aware of the breach
- Individuals affected by the breach must be notified as soon as possible
- Your organisation must have robust measures in place to recognise a personal data breach and a well-prepared response plan in place
- A dedicated person or team should be allocated for the responsibility of breach management

Penalties for Non-Compliance

- Organisations which do not comply with the new GDPR regulations can expect to see a substantial increase in fines
- The maximum fine will be 4% of organisation's gross global revenue or €20 million, whichever figure is greater
- Organisations with measures in place to comply with GDPR can expect considerably lower fines

Digital Marketing and GDPR

The ICO have highlighted the following points as key changes regarding consent – all of which need to be integrated into your digital marketing campaign.

Active opt-in – the use of pre-ticked boxes will no longer be acceptable. Users will be required to actively opt-in via means of a tick box, slider or similar methods.

Unbundled – Requests for consent must be separate from other terms & conditions

Opt out option – Users have the right to withdraw consent at any time, this should be made easy and straightforward

Granular – Granular options should be available wherever possible, in order for users to consent separately for different types of processing

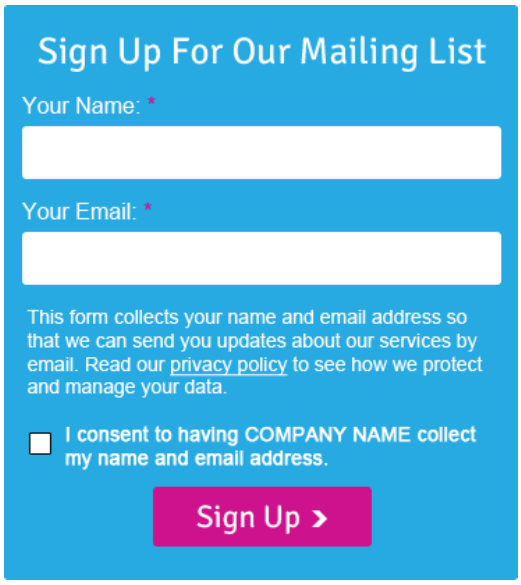
Named – Your organisation must be clearly named, as well as any third parties such as Google Analytics or Mailchimp

Recording consent – A record must be kept of exactly how your organisation obtained consent and for what purposes

How to Comply – Suggested Best Practices for Websites

Email Marketing – Gaining Consent to Send

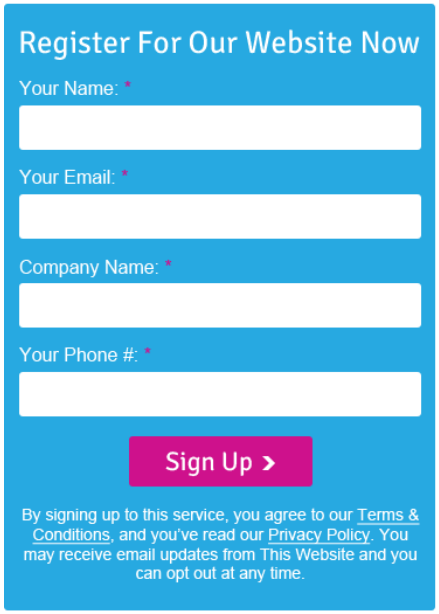
If your organisation wants to send marketing emails, they must have consent. The request for consent should be clearly labelled, as well as clarifying that email marketing is optional. It will also require the user to actively opt-in. Additional consent will be required for the use of Third Party email marketing services such as Mailchimp or Campaign Monitor. For example:



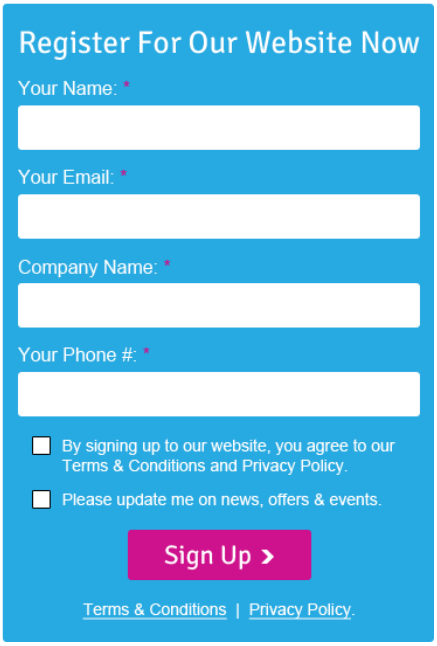
Website Registration Forms

If your organisation requires users to register to use your services, consent will be required. The following form asks the user to actively opt-in and read through the terms & conditions, these are "unbundled". Registration will not be possible without an active opt-in. For example:

Non-Compliant Example



Compliant Example



Email Marketing – Double Opt-In

Regardless of the method of email marketing signup, it is recommended to use double opt-in for email marketing purposes. A double opt-in process requires the user to fill out an initial consent form, which upon completion generates an auto-response email asking the user to confirm that he/she actively joined your email list.

Ecommerce Websites and Data Collection

If you run an ecommerce website, you are likely to be using an external payment gateway for any transactional information. However, if your website is collecting personal information such as name, email address, phone number and delivery address, then new processes will need to be put into place.

There are often two ways users can complete a transaction on a website:

1. A user has consented to register to your website and has an account with you
2. A user can checkout as a guest

If you offer a guest checkout, and a Data Subject doesn't have an account on your website, then you will need to modify your processes to remove any personal information after a reasonable period, for example, 60 days. GDPR legislation is not explicit about the set number of days, and it is down to you to define what is reasonable and necessary. This change will generally require development to be carried out on your website to ensure that guest accounts are removed on a regular daily cycle, as per your policy – Siruss can advise on the requirements for this irrespective of your ecommerce platform.

In light of the suggestions for compliance for both consenting registrants and guests, to suggest that perhaps a visitor to your ecommerce store should not be allowed to checkout at all until a checkbox is ticked confirming they have understood your privacy policy and terms and conditions.

Ecommerce Websites and Email Consent at Checkout

It is common practice to have a checkbox in the checkout where users can opt-in to email marketing. As with the Website Registration Forms example above, the terms and conditions and email opt-in have to be "unbundled" and boxes cannot be pre-checked. Depending on your e-commerce platform, this may require additional development to be implemented.

The Right to Withdraw/Remove Data

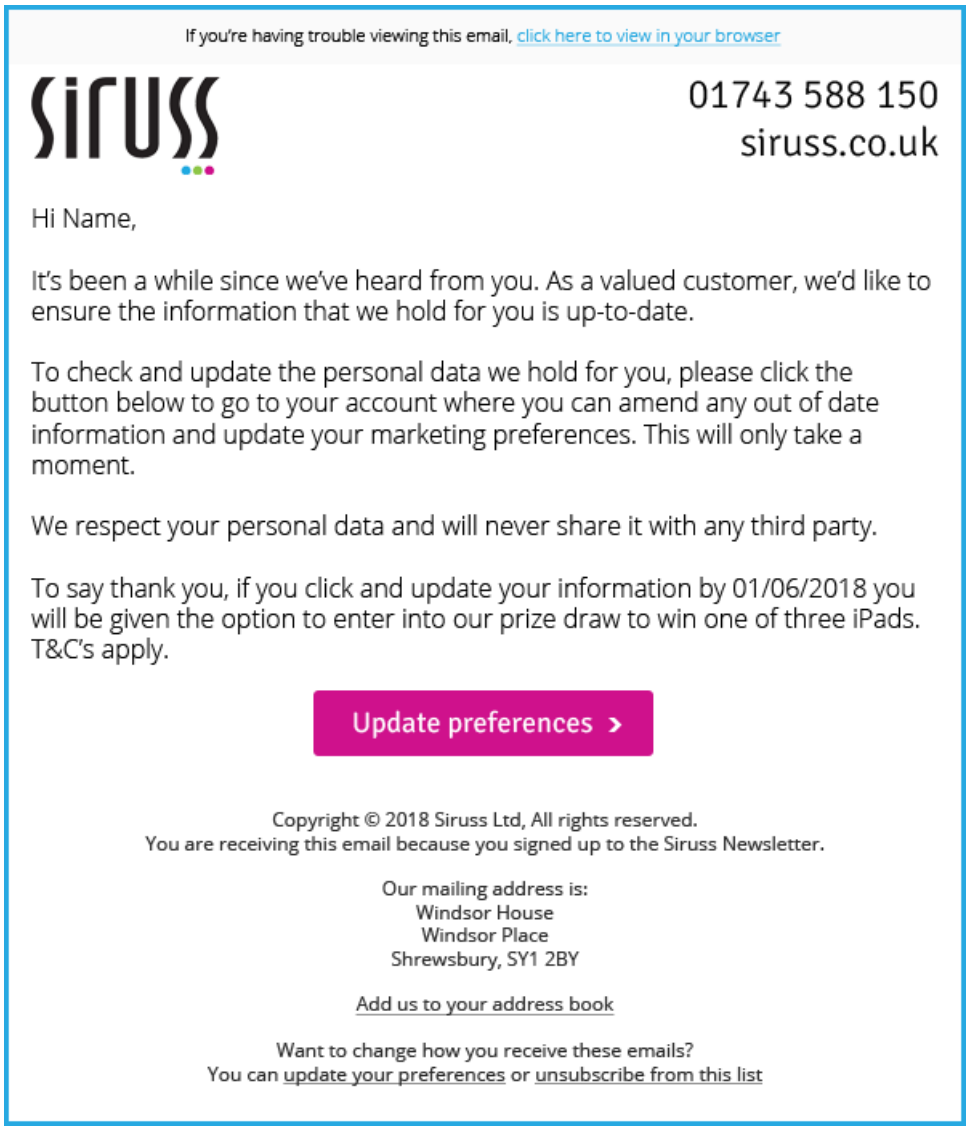
Users have the right to withdraw consent, unsubscribe to any particular service and request that their personal data be deleted. Your organisation should have a process in place which makes this simple and straightforward. Providing your clients with a dedicated opt out page with granular options for the user to be able opt-out should they wish, is an effective way of addressing this concern. The ability to opt out should be easily accessible via a clearly visible link, such as in the footer of your website, and in any email marketing.

Editing Personal Details – The Right to Rectification

In some cases, a user may wish to edit or rectify the data an organisation holds about them – a clear and simple process should be in place ideally with the use of a contact form.

Refreshing Consent

It is good practice to keep consent refreshed and up to date. This also provides the user with the opportunity to update their information or withdraw consent should they wish to. For example:



If you're having trouble viewing this email, click here to view in your browser

SIRUSS

01743 588 150
siruss.co.uk

Hi Name,

It's been a while since we've heard from you. As a valued customer, we'd like to ensure the information that we hold for you is up-to-date.

To check and update the personal data we hold for you, please click the button below to go to your account where you can amend any out of date information and update your marketing preferences. This will only take a moment.

We respect your personal data and will never share it with any third party.

To say thank you, if you click and update your information by 01/06/2018 you will be given the option to enter into our prize draw to win one of three iPads. T&C's apply.

Update preferences ›

Copyright © 2018 Siruss Ltd, All rights reserved.
You are receiving this email because you signed up to the Siruss Newsletter.

Our mailing address is:
Windsor House
Windsor Place
Shrewsbury, SY1 2BY

Add us to your address book

Want to change how you receive these emails?
You can update your preferences or unsubscribe from this list

The Use of Third Party Providers

Users must also consent to the use of, or collection of their data by any Third Party providers. Separate consent should be given for each Third Party, in the case of more than one.

Your organisation is responsible for actions taken by any Third Party providers – it is important to identify all Third Party providers, understand what data they collect, store and process and if they are GDPR compliant.

Google Analytics and GDPR

Google have a privacy compliance section, with reference to GDPR here:
https://privacy.google.com/businesses/compliance/#?modal_active=none

They're currently working on GDPR compliance, but other information is sparse at this stage.

While their information doesn't specifically focus on their Analytics software directly, it is an anonymous tracking system which is likely to not be impacted by GDPR. It is wise to reference Google Analytics in your Privacy Policy if you don't already.

Privacy Policy

Your organisation's Privacy Policy is the best place to disclose all required information regarding data collection and storage, stating how personal data will be stored, for what length of time and exactly how it will be used. Every purpose of usage of personal data collected from your users should be identified, described and justified within the privacy policy. See Appendix 1 for more details.

Terms & Conditions

Terms & Conditions should be a separate document away from the Privacy Policy and may also require reviewing.

Examples of What Not to Do

The ICO has compiled a document citing examples of good and bad privacy notices. This is available to all organisations for reference purposes.

https://ico.org.uk/media/for-organisations/documents/1625136/good-and-bad-examples-of-privacy-notices.pdf

How Siruss Can Help

Creating a framework in which privacy is forefront within your organisation may involve the implementation of some technical adjustments. The Siruss development team can work with your organisation to help prepare it for GDPR by creating consent forms, a specific opt-out page, parental controls and adapting your website to highlight the options for consent and withdrawal of consent to suit your organisation's requirements.

Ways to Obtain Consent

- Ticking an electronic opt in box
- Selecting from prominent Yes/No options
- Filling in a form
- Responding to an email request
- Signing a consent form on paper
- Oral consent

Requesting Consent

The following information must be included in all consent requests as a minimum:

- The name of your organisation and any third parties
- Why you want the data and what you will do with it
- Information informing the subject of their right to withdraw consent at any time

Remember

- Users must be required to actively opt in
- Consent must prominent and unbundled (separate from other terms and conditions)
- Clear, easy to understand language should be used, not legal jargon
- Granular options to give separate consent for different purposes and different types of processing must be used wherever possible
- All details of consent should be recorded to evidence
- Keep consents under review and regularly refresh them

What Needs to Be Displayed to the User?

Data Subjects should be easily able to do the following:

- Access their personal data

- Have their personal data erased if they choose to do so
- Be able to correct any inaccuracies regarding their personal data
- Prevent automated decision making and profiling
- Data portability

Your company must be able to demonstrate that consent has been obtained in a lawful process.

Contact Siruss

Phone: 01743 588 150

Email: info@siruss.co.uk

More info on GDPR: https://www.siruss.co.uk/gdpr

Appendix 1

The following table taken from the ICO website, illustrates what needs to be included in your privacy policy – more information can be found at: https://ico.org.uk/media/for-organisations/data-protection-reform/overview-of-the-gdpr-1-13.pdf

What information must be supplied?	Data obtained directly from Data Subject	Data not obtained directly from Data Subject
Identity and contact details of the controller and where applicable, the controller's representative and the data protection officer.	Yes	Yes
Purpose of the processing and the legal basis for the processing.	Yes	Yes
The legitimate interests of the controller or Third Party, where applicable.	Yes	Yes
Categories of personal data.	No	Yes
Any recipient or categories of recipients of the personal data.	Yes	Yes
Details of transfers to third country and safeguards.	Yes	Yes
Retention period or criteria used to determine the retention period.	Yes	Yes
The existence of each Data Subjects rights.	Yes	Yes
The right to withdraw consent at any time, where relevant.	Yes	Yes
The right to lodge a complaint with a supervisory authority.	Yes	Yes

The source the personal data originates from and whether it came from publicly accessible sources.	No	Yes
Whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the correct personal data	Yes	No
The existence of automated decision making, including profiling and information, about how decisions are made, the significance and the consequences.	Yes	Yes
When should information be provided?	At the time the data are obtained.	Within a reasonable period of having obtained the data (within one month). If the data are used to communicate with the individual, at the latest, when the first communication takes place; or If disclosure to another recipient is envisaged, at the latest, before the data is disclosed.

Further Reading:

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