silkmoth

DATA PROTECTION AND THE GDPR

INTRODUCTION

Data protection laws have changed. The General Data Protection Regulation (GDPR) is already in force and we are currently in a period of implementation with a deadline for compliance of 25th May 2018.

As part of our commitment to our customers, we have created this guide to explain GDPR and how you should approach this change in legislation.

All of our customers are different and there isn't a *one size fits all* approach to GDPR compliance. This guide covers some of the commonly asked questions and provides links for further guidance and information.

GLOSSARY

Data Subject	A living individual / natural person
Personal Data	Any information relating to an identified or identifiable data subject. Data subjects can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location, online identifier (e.g. IP address) etc.
Special Category Data	Personal data revealing: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade-union membership • Data concerning health, sex life or sexual orientation • Genetic data • Biometric data
Processing	Any operation performed upon personal data such as collection, recording, organisation, structuring, storage, alteration, retrieval etc.
Data Controller	The natural or legal person, public authority, agency or any other body which determines the means of the processing of personal data. In most instances, where Silkmoth process personal data, it is done so under the instructions of our customers. Silkmoth's customers are data controllers.
Data Processor	The natural or legal person, public authority, agency or any other body which processes personal data on behalf of the data controller. Silkmoth is a data processor.
Consent	Any freely given, specific, informed and unambiguous indication of a data subject's wishes that signifies agreement to personal data being processed. The data subject gives consent by a statement or clear affirmative action.
Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

YOUR RESPONSIBILITIES

The GDPR applies to all data controllers and data processors. If you collect any personal data in running your business (which you almost certainly will) then the GDPR applies to you.

FAIR, LAWFUL AND TRANSPARENT PROCESSING

Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.

PURPOSE

Personal data may only be collected for specified, explicit and legitimate purposes and must not be further processed in a manner that is incompatible with those purposes.

MINIMISATION

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which those data are processed.

ACCURACY

Personal data must be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate are either erased or rectified without delay.

RETENTION

Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

SECURITY

Personal data must be processed in a manner that ensures appropriate security of those data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

ACCOUNTABILITY

The controller is responsible for, and must be able to demonstrate compliance.

KEY CHANGES TO DATA PROTECTION LEGISLATION

MORE COMMUNICATION

You will need to give people more information about what you collect and what you do with their data at the point you collect it.

SUBJECT ACCESS REQUESTS

Requests for copies of personal data from individuals (subject access requests) will need to be responded to within one calendar month. It is no longer possible to make any charge for dealing with a subject access request.

OBLIGATIONS

There are direct obligations on data processors as well as on data controllers. If you use a third party, like Silkmoth, to process personal data then you should have a written contract (data processor agreement) in place.

FINES

Currently the highest fine the Information Commissioner's Office (ICO) can levy is £500,000. From 25th May 2018 the ICO can issue fines up to €20 million or 4% of your global annual turnover (whichever is the higher) for serious data breaches.

CONSENT

Consent will be much harder to achieve. If you rely on consent from individuals to use their personal data in certain ways, for example to send marketing emails, there are additional requirements to comply with.

RETENTION

Retention policies need to be clear. You cannot keep data for longer than is necessary for the purpose for which it was collected. You also need to inform people how long you will keep their personal data. You cannot keep personal data indefinitely.

PRIVACY BY DESIGN

If you are planning to put in place a new system or website that will capture and process personal data then you should consider whether the service provider you choose has adequate security to protect personal data.

DATA BREACHES

You only have 72 hours from being aware of a data breach to report it to the ICO.

CHILDREN

There are additional protections for children's personal data (i.e. under the age of 16). If you collect children's personal data then you need to make sure that your privacy policy is written in plain, simple English. If you offer an online service to children, you may need to obtain consent from the parent or guardian to process the personal data.

ARE YOU READY?

Silkmoth's tips for GDPR readiness are:

PROCESS

Understand the journey that personal data takes through your business. You should review and identify:

- What personal and special category data you collect/hold;
- Where you get such data from;
- Where you send this data;
- Who you share data with;
- What you tell people when you collect it;
- What your legal basis for processing is;
- How you secure the data; and
- How you dispose of the data when you no longer need it.

This will allow you to identify areas of risk.

AWARENESS

Make sure that your employees are aware of the GDPR and data protection issues and that they know who to talk to if they receive a subject access request or if there is a breach.

POLICY

Make sure the policies and procedures you have in place help your employees deal with data protection issues.

Silkmoth's data protection policy is shared here:

https://www.silkmoth.com/documents/data-protection-policy.pdf

COMMUNICATION

Make sure you tell individuals at the point of collection what you will do with their data and when you will delete it.

ICO GUIDANCE

Take a look at the *12 steps to take now* guide produced by the ICO.

https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf

Also work your way through the Data Protection self-assessment tools.

https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/getting-ready-for-the-gdpr/

STEPS TO TAKE ON YOUR WEBSITE

It's quite likely that you have received this guide because Silkmoth run a website for your business. To ensure your website is GDPR compliant we recommend you take the following steps.

1. Review your privacy policy
   An example of a GDPR compliant privacy policy can be found here:

   https://www.silkmoth.com/privacy

2. Review the data your website holds
   Silkmoth have already carried out a review of the data held by all of the websites and services we operate. Get in touch and we can supply you with a list of personal data that we process on your behalf.

3. Review your consent capture
   At the point where you capture personal data (e.g. during an e-commerce checkout process) you must ensure that the data subject understands how their data will be used. You may need to allow individuals to give consent to some forms of usage but not others.

4. Put a data processor agreement in place
   As a data controller you should have a written contract in place with any third-party data processor you use. You can download Silkmoth's standard data processor agreement here:

   https://www.silkmoth.com/documents/template-dpa.docx

5. Use HTTPS
   You will have noticed recently that Silkmoth have migrated your website(s) to new, more secure servers and, where appropriate, upgraded the connection to use HTTPS. This is an encrypted protocol meaning that all data transmitted between the visitor and your website is secure.

CONTACTS

If you have any questions please do not hesitate to get in touch:

Carl Dean
Managing Director
E: carl.dean@silkmoth.com
T: 01625 433388

Simon Cooper
Data Protection Officer
E: simon.cooper@silkmoth.com
T: 01625 433388