Lesniak Swann
Unfair competitive advantage

GDPR Compliance Statement

Introduction

The General Data Protection Regulation (GDPR) is a new EU law which affects all organisations that hold and process the personal data of EU citizens.

In compliance with the General Data Protection Regulation (GDPR), we are responsible for protecting the personal data we collect from our clients upon sign up (name, email, address, password, billing data). We must also ensure that our clients' data hosted on our servers during their usage of our services is also protected. We collect, store and work with our clients' data in a legitimate way and we want to inform you of how we do this. We would also like to provide transparency as a processor on the way we store the data our clients host on our servers.

Our Commitment

Lesniak Swann are committed to ensuring the security and protection of the personal information that we process, and to provide a compliant and consistent approach to data protection. We have always had a robust and effective data protection program in place which complies with existing law and abides by the data protection principles. However, we recognise our obligations in updating and expanding this program to meet the demands of the GDPR and the Data Protection Bill.

We are dedicated to safeguarding the personal information under our remit and in developing a data protection regime that is effective, fit for purpose and demonstrates an understanding of, and appreciation for the new Regulation. Our preparation and objectives for GDPR compliance have been summarised in this statement and include the development and implementation of new data protection roles, policies, procedures, controls and measures to ensure maximum and ongoing compliance.

How we prepared for GDPR

Lesniak Swann already have a consistent level of data protection and security across our organisation, however it was our aim to be fully compliant with the GDPR by 25th May 2018.

Our preparation includes:

Information Audit

We have carried out a company-wide information audit to identify and assess what personal information we hold, where it comes from, how and why it is processed and if and to whom it is disclosed.

Policies & Procedures

Revised existing data protection policies and procedures to meet the requirements and standards of the GDPR and any relevant data protection laws, including:

- **Data Protection** – our main policy and procedure document for data protection has been overhauled to meet the standards and requirements of the GDPR. Accountability and governance measures are in place to ensure that we understand and adequately disseminate and evidence our obligations and responsibilities; with a dedicated focus on privacy by design and the rights of individuals.
- **Data Retention & Erasure** – we have updated our retention policy and schedule to ensure that we meet the 'data minimisation' and 'storage limitation' principles and that personal information is stored, archived and destroyed compliantly and ethically. We have dedicated erasure procedures in place to meet the new 'Right to Erasure' obligation and are aware of when this and other data subject's rights apply; along with any exemptions, response timeframes and notification responsibilities.
- **Data Breaches** – our breach procedures ensure that we have safeguards and measures in place to identify, assess, investigate and report any personal data breach at the earliest possible time. Our procedures are robust and have been disseminated to all employees, making them aware of the reporting lines and steps to follow.
- **Subject Access Request (SAR)** – we have revised our SAR procedures to accommodate the revised 30-day timeframe for providing the requested information and for making this provision free of charge. Our new procedures detail how to verify the data subject, what steps to take for processing an access request, what exemptions apply

and a suite of response templates to ensure that communications with data subjects are compliant, consistent and adequate.

- **Legal Basis for Processing** – we have reviewed all processing activities to identify the legal basis for processing and ensuring that each basis is appropriate for the activity it relates to. Where applicable, we also maintain records of our processing activities, ensuring that our obligations under Article 30 of the GDPR and Schedule 1 of the Data Protection Bill are met.
- **Privacy Notice/Policy** – we have reviewed our Privacy Notices to comply with the GDPR, ensuring that all individuals whose personal information we process have been informed of why we need it, how it is used, what their rights are, who the information is disclosed to and what safeguarding measures are in place to protect their information.
- **Obtaining Consent** – we have revised our consent mechanisms for obtaining personal data, ensuring that individuals understand what they are providing, why and how we use it and giving clear, defined ways to consent to us processing their information. We have developed stringent processes for recording consent, making sure that we can evidence an affirmative opt-in, along with time and date records; and an easy to see and access way to withdraw consent at any time.
- **Direct Marketing** – we have revised the wording and processes for direct marketing, including clear opt-in mechanisms for marketing subscriptions; a clear notice and method for opting out and providing unsubscribe features on all subsequent marketing materials.
- **Processor Agreements/Supplier Validation** – where we use any third-party to process personal information on our behalf (i.e. Payroll, Recruitment, Hosting etc), we have secured Processor Agreements to ensure that they (as well as we), meet and understand their/our GDPR obligations. These measures include initial and ongoing reviews of the service provided, the necessity of the processing activity, the technical and organisational measures in place and compliance with the GDPR. In addition we have contacted our existing suppliers to ensure that they are complying with the law and have incorporated appropriate GDPR audit compliance questions into our Supplier Questionnaires for new Suppliers.
- **Special Categories Data** – where we obtain and process any special category information, we do so in complete compliance with the Article 9 requirements and have enhanced protection on all such data. Special category data is only processed where necessary and is only processed where we have first identified the appropriate Article 9(2) basis or the Data Protection Bill Schedule 1 condition. Where we rely on consent for processing, this is explicit and is verified by a signature, with the right to modify or remove consent being clearly signposted.

Data Subject Rights

In addition to the policies and procedures mentioned above that ensure individuals can enforce their data protection rights, we provide easy to access information via our website, in the office, during induction of an individual's right to access any personal information that Lesniak Swann processes about them and to request information about:

- What personal data we hold about them
- The purposes of the processing
- The categories of personal data concerned
- The recipients to whom the personal data has/will be disclosed
- How long we intend to store your personal data for
- If we did not collect the data directly from them, information about the source
- The right to have incomplete or inaccurate data about them corrected or completed and the process for requesting this
- The right to request erasure of personal data (where applicable) or to restrict processing in accordance with data protection laws, as well as to object to any direct marketing from us and to be informed about any automated decision-making that we use
- The right to lodge a complaint or seek judicial remedy and who to contact in such instances

Information Security & Technical Measures

Lesniak Swann takes the privacy and security of individuals and their personal information very seriously and take every reasonable measure and precaution to protect and secure the personal data that we process. We have robust information security policies and procedures in place to protect personal information from unauthorised access, alteration, disclosure or destruction and have several layers of security measures, including:

- Remote access to systems and data is over an SSL encrypted connection
- Users only have access to data they need for their role

- Having a complex password policy in place

GDPR Roles and Employees

Lesniak Swann have designated Alex Swann as our Data Protection Lead and have appointed a data privacy team to develop and implement our roadmap for complying with the new data protection Regulation. The team are responsible for promoting awareness of the GDPR across the organisation, assessing our GDPR readiness, identifying any gap areas and implementing the new policies, procedures and measures.

Lesniak Swann understands that continuous employee awareness and understanding is vital to the continued compliance of the GDPR and have involved our employees in our preparation plans. We have implemented an employee training program specific to the which will be provided to all employees, and forms part of our induction and annual training program.

Handling Client Data

Terms of Service And Privacy Policy Updates

The GDPR says we have to inform clients what data we collect about them and legitimise how we use it afterwards. We only collect a minimal amount of personal data that is required to deliver the hosting service to your company. We collect your physical address for invoicing and tax purposes, your email address to contact you about our service, orders and important information relating to your business with us. We never use any of the data collected for profiling, secondary purposes and we do not sell it to anyone.

In conformance with the GDPR requirements, our new Privacy Policy will fully describe why and how we collect and process your personal information. As our client you can validate that we handle this information carefully and responsibly.

External Service Provision

Some of the services we provide customers include services from external partners, such as Digital Ocean, Rackspace, Amazon, TSOHost, MailChimp, SendGrid. Some but not all of these services either require client data, or that client data is stored in a secure password encrypted file (i.e. in the case of backups).

Internal Procedures and Access-Control

In line with the GDPR we are auditing and enhancing our security, access control and data storage provision. We are adding new procedures where this is required by the new regulation. For example, we are implementing higher levels of security authentication for sensitive data and access control we have to third party companies used by the client, i.e. Domain Registrars and Mailchimp.

Mitigating Data Breach, Our Commitment to System Security

We work closely with Digital Ocean for the server management and monitoring of our web servers.

Through our server management policies we closely monitor any unauthorised system access and we put multiple preventive measures into action to mitigate the risks of cyber attack. Server systems are regularly updated for this purpose. Some sites also feature an auto-banning protection system actively blocking users/IPs which are detected as behaving against defined rules.

We implement a level of security deemed appropriate for the site we are managing based on our experience. However, if a client requests a higher level of security, such as 2-factor authentication on their website, IP blocking, etc. we can provide a tailored security solution appropriate to their data needs.

Data Protection by Design and Data Protection Impact Assessments

Security and protection of clients data is our primary priority. Whenever we develop a new system, security comes as the first design principle of the architecture of a system. Our first goal is to protect the integrity of the new production system. Our second goal is to protect the customer data that is being stored and used by that system.

New Data Processing Agreement

Many of our clients operate using the personal data of their own customers. For example, they take orders, they collect emails through sign up forms, they process credit cards, and more. Our client controls their customers' data and how this data gets collected and used. Lesniak Swann stores this data on our servers and therefore takes part in its processing. The new data processing agreement will regulate our processing of that data only for the purposes of delivering the hosting service and resolving technical inquiries and no other secondary functions. This has always been the case. In providing services to our customers we are committed to being a trusted partner, adhering to the principles of transparency, and meeting our obligations under GDPR adequately.

Right to be Forgotten

Under the GDPR every client can request "to be forgotten", meaning all their data has to be deleted and never used again, except in certain circumstances, which may include having to keep processing your personal information to comply with a legal obligation. An example of such obligation is the requirement to keep a copy of all invoices to comply with financial and tax legislation. We will comply and act on our clients' right to be forgotten via written communication to alexs@lesniakswann.com

Privacy Policy

We are developing a new Privacy Policy to detail how we process your personal data. As a client we will provide transparency on the data we store about you, how you can update it and, where we rely on your consent for processing the data, you can withdraw your consent to that use. Our use of your personal information is necessary to perform our obligations under our service provision to you. We currently do not send marketing information or promotional offers but if we were to do so in the future we would ask for your specific consent.
