GDPR compliance

Overview

On 25 May 2018 the European wide General Data Protection Regulation (GDPR) will come into effect. This regulation places specific emphasis on the handling and protection of personal data and applies to all the countries of the European Union.

The regulation outlines six key principles for organisations that process individuals' personal information. These are that data shall be:

- Processed lawfully, fairly and transparently
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary for processing
- Accurate and kept up to date
- Retained only for as long as necessary
- Processed in an appropriate manner to maintain security

JS2 has taken steps to ensure that the GDPR requirements have been reviewed in the context of our business, communicated to all staff and complied with in full.

We only process client data in line with the engagement requirements and our data protection policy. We take the protection of all client data extremely seriously and we have implemented data security controls consummate with the sensitivity of this data as shown below.

JS2 does not process special category data.

If a breach were to occur we will take steps to respond to such instances in line with the requirements of the GDPR.

JS2 does not store any data outside the European Union.

Data collected

None of our clients are individuals but we collect personal data in the course of our work relating to employees, trustees, suppliers and customers of our current, past and prospective business clients.

Information collected may include:

- Full name and title
- Home address
- Date of birth
- National Insurance number
- Email address
- Mobile and home telephone numbers
- PAYE tax code
- Bank account details

Clients provide most of the data directly to us either in paper or electronic format. Some data is also provided by third parties e.g. HMRC, Companies House or other accountants when they provide professional clearance and transfer of information on change of appointment.

We collect, use, disclose and store personal data in order to operate our business and provide services to clients. We do this for any client that has requested services from us and where we have agreed to provide such services in our engagement letters, proposals, correspondence or verbal agreements. We only collect data that we actually need and only for the above purposes.

Individuals may object to us collecting certain data about them. If information is not provided we may not be able to undertake the services that we have contracted to provide.

Use of client data

Client data is only used for the purpose for which it was collected. Client data is processed lawfully as a means to provide services to our clients.

We rely on the lawful basis as to why we obtain and process client data and specific consent is generally not required. Our lawful basis is that processing of data is necessary for the performance of a contract with a client or to take steps to enter into a contract or that processing is necessary for compliance with a legal obligation.

We do not undertake general direct marketing to our clients. We use client data to communicate with our clients in order to provide agreed services.

We do not share client data with third parties for marketing purposes.

We do not share or pass client details to another organisation unless this is required as part of our agreed services. The main organisations that we will provide such details to are HMRC and Companies House.

Data retention

We retain personal information for as long as we reasonably require it for legal or business purposes. In determining data retention periods we take into consideration laws, contractual obligations and the expectations of our clients. When we no longer need personal information we delete or destroy it in a secure manner.

Data security

JS2 is committed to protecting the confidentiality, integrity and availability of personal and client data. A risk register is maintained and is reviewed annually and the overall security of all data considered as part of this.

The controls we have in place to protect it are detailed below.

Information security policy and management

All staff, regardless of their role, are responsible for conducting their work in a manner that protects the security of the client data and for complying with the security principles below. The management team are responsible for the implementation of all policies and for ensuring the adherence by all staff. The policies are under continual review as guidance is updated and regular updates are provided to all staff.

Security monitoring and security incident management

It is the responsibility of all staff to identify any data breach that might occur and to report this to the management team. Our organisational security policy implements a breach management plan

based on the four key elements of containment and recovery, risk assessment, notification and evaluation and response.

Data backup and Disaster recovery

Backups are part on premises and part cloud based. All major servers are backed up daily to full image file. The images are stored on a local NAS appliance and typically there would be around 3 months of backups available. A Barracuda Backup Appliance backs up file system data / client data and accounting software data and exchange email data on a real time basis. The data on this device is then further replicated offsite to an unlimited cloud storage account associated with the Barracuda backup service held in Europe, on a nightly basis.

The Symantec backups are capable of 'new metal' restore so in the event of complete server failure can be rapidly restored to new hardware. The offsite Barracuda backups contain all mission critical data that would be required in the event of a total loss of the onsite equipment. Granular restores are available making data fast to access should the need arise. A full server rebuild from the onsite back up would be achieved within 24 hours and using offsite data an operational state should be achieved within 48 hours, on a best endeavours basis.

Daily monitoring of all backups is carried out and problems resolved immediately and backups re run in the event of failure.

Digital Data Security

Access to the network is protected by an SSL VPN appliance as well as an RDP server which uses two factor authentication for all client logons. Access can only be gained by authorised users.

Client access on the RDP servers is restricted to client specific data only.

Perimeter firewall is protected through a network security device. Streaming proxies are enabled that include intrusion prevention, Gateway anti-virus & Gateway anti-spyware. A web blocker is deployed to control access to web sites.

End point security advanced antivirus protection is deployed on every device including servers.

E-mail is protected by Barracuda ESS cloud security services both inbound and outbound also offering full encryption capability . Work mobile phones include device management software that enables the phone to be located, locked and erased, should a phone be lost.

No general access is allowed to USB data sticks within the network and all laptops have full disk encryption.

Personnel and security awareness

We aim to embed data protection in our firm culture and all staff are receiving an update to raise awareness of GDPR and their responsibilities. All staff are required to comply with our Data Protection and Computer policies, which are also in the process of being reviewed.

Physical, environmental and communications security

JS2 offices are on the third floor of an all glass secure building in the town centre of Woking. A fully manned building reception is in place during working hours and access to the building is controlled by an access control mechanism out of hours. JS2's office has an independent access control mechanism which controls access to our office out of office hours to appropriate staff.

CCTV cameras are in place within the office to monitor all entrances and exits, our IT server and the storage of secure data.

Filing cabinets and cupboards are locked overnight , wherever practicable, and a safe is used for specific information.

Digital data is transferred to and from clients using secure cloud workspaces, password protection and email encryption as appropriate.

Contacting us

If you would like to contact us about GDPR, data protection or how we handle your data in general, please send an email to info@js2.net and we will get back to you as soon as possible.