Prodigy IT Solutions GDPR Statement

Introduction

The new EU General Data Protection Regulation (GDPR) comes into force on 25th May 2018 and will impact every organisation which processes personal data of EU citizens. It introduces new responsibilities, empowers businesses to be accountable for their processing of personal data as well as enabling EU citizens to protect their privacy and control the way their data are processed. Even though the UK will be leaving Europe, the GDPR still applies and will replace the UK's Data Protection Act 1998 when it comes into force.

Data protection definitions

Personal data is any information that relates to a living individual. It also includes any data that can be used with other sets of data to identify an individual. Typical examples of personal data are: name, identification number, location data, online identifier, email address, etc.

Processing relates to any operation carried out on personal data including collection, recording, organising, structuring, storing, using, etc. Processing also doesn't have to be by automated means which means that processing includes paper-based, non-digital systems.

A **Data Subject** is the individual whose personal data is being processed

A **Data Controller** is the organisation which determines how personal data is processed

A **Data Processor** is an organisation which processes data on behalf of a Controller. This typically means a third party who is used by the Controller to process their data (e.g. a marketing company used to send out marketing materials)

For detailed information about the GDPR and data protection, visit the Information Commissioner's Office website: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

Your GDPR responsibilities

When you use our services to store or process your personal data (including customer's or user's data), you are the Data Controller and we are a Data Processor. This will be true for any personal data you place on our servers either directly, via a hosted website or by use of any of our other services.

The GDPR requires you, as a Data Controller, to ensure that any Data Processor services you use to process personal data are GDPR compliant. This means that when you use any of our services to process your personal data you need to carry out due diligence on our services and ensure certain contractual terms are in place.
This GDPR statement is our way of helping you meet these GDPR regulatory requirements and to offer you assurance that we take GDPR and the security of your personal data as part of the everyday running of our services.

Our GDPR commitment

As a UK company, we are committed to ensuring our business, services and internal processes are GDPR compliant. We have used a consultant to advise us on elements of our services and how the GDPR changes impact our compliance. As such, this GDPR Statement provides our assurances to GDPR compliance.

By the GDPR implementation deadline, we will have put in place:

- Employee data protection training to ensure all staff understand their role in data protection compliance
- Updated internal policies relating to data protection and responsibilities within our businesses for ongoing GDPR compliance
- Checks of all our systems, processes and services to ensure they meet the requirements of GDPR, particularly around security of data and our use of any external third-party services
- Processes to ensure ongoing compliance past the GDPR deadline
- Updated terms and conditions of services that meet the contractual requirements of GDPR in the Data Controller – Data Processor relationship

Our services are compliant because:

- We have fully assessed our own GDPR compliance both in terms of the services we offer to our customers but also in terms of our own internal policies and procedures
- We have appropriate technical and personnel protocols in place to ensure the security of your data
- We carry out due diligence against any sub-processors or other third-party processors we use to ensure their GDPR compliance (such as data centres)
- We only allow specific members of staff access to our servers and what access that is available, is limited to specific circumstances
- We do not transfer your data outside the EEA (all our services are hosted in the UK)
- Our staff are trained in GDPR compliance and understand their responsibilities for managing the systems that process your personal data

Our role as a Data Processor

You are the owner of the data you submit to our services (whether they are hosted on your premises or on our servers).

When your data is placed on our servers, you are the Data Controller and we are the Data Processor. We do not access the data you store on our services unless you request otherwise and any processing (as a Data Processor) is only in terms of the hosting services we provide to you. We do not use your data for any processing of our own.

We do not share or provide access to any of your data with third parties unless required to do so by law. Where law enforcement or other authorised parties request access to our servers, we follow strict internal policies for dealing with such requests in line with existing

UK law. Furthermore, the third parties are required to demonstrate they have a lawful reason to access the data and under what authority.

Data location

Data-centre in Bournemouth, UK. Using physical servers owned by us.
Data-centre in Blandford, UK. Using physical servers owned by us.
Cloud services in London, UK. Using Amazon Web Services.
Cloud services in London, UK. Using Microsoft Azure.
Cloud Services in Cardiff, UK. Using Microsoft Azure.

Security

Maintaining security

All our employees keep up to date with all technical aspects of security and ensure the ongoing security of our servers and systems. This means that any security patches are applied to our systems as a matter of priority and any changes or updates to our own systems are done so, always, with data protection and privacy in mind and where appropriate, in discussion with our customers. Where we have an agreement in place with our customers to do so, we also maintain the security of our customer's own servers or hosted applications.

All servers are locked down and pass PCI certification requirements.

Access to servers

Remote admin access to our servers is strictly restricted to key personnel within our business. Currently the following key personnel that have access are our support technicians for the purposes of being able deliver the service to you.

Data centre staff have physical access to the servers, but we have strict protocols in place to ensure they only do so, if requested by a member of our technical support team and such a request will only be in cases when they need to carry out a visual check of a server or carry out maintenance on the server itself.

Our employees

All our employees are trained and made aware of their responsibilities under GDPR. This includes their responsibilities with regards to access, security and processing of any personal data stored on our servers.

Security and data governance are covered in our employee handbooks, internal policies and actively discussed as part of our monthly meetings to ensure all staff are up to date.

Third party services

Other than the data centres who host our servers, we do not use any third party suppliers or services that would have access to, or process, any data you process on our servers.
Strict protocols (as set out above) are in place regarding data centre staff access to our servers.

Changes to our approach

Should our approach to any aspect covered by this statement change we will make sure, where your data is impacted, we notify you within a reasonable timeframe and in line with any contractual terms in place between us.

Data breaches

In the unlikely event of a breach occurring (as defined in the GDPR) we will notify you within 48 hours of the breach coming to our attention. This will be enough time for you to consider your requirements, under GDPR, for reporting the breach to the ICO and Data Subjects.

We help you to comply with GDPR

Our approach to our own compliance also helps you comply with your own GDPR compliance requirements. This statement should go some way to explain our approach to GDPR compliance. By using our services, you can be assured that your use is GDPR compliant.

Furthermore, if required we will assist you or the Information Commissioner's Office with any query relating to the GDPR compliance of our services.

Data protection contact

Any questions, queries or requests for further information regarding our GDPR compliance should be sent to:

Email: gdpr@prodigyitsolutions.com
or
Address: Prodigy IT Solutions, Everley, Blandford, Dorset, DT11 8PT