Data Protection Framework

Understanding the Data We are Protecting

The first step in protecting the data is understanding the data you are trying to protect. The first step in our process to data protection is to identify the data we needed to protect, understand why we were storing the data, and map out how the data transfers through our systems and processes. Blue Marble Payroll regularly and frequently audits the personal data we collect and Data Mapping and Categorization

- Onboarding Data Flow
- Data Flow
- Sales and Marketing Data Flow
- System Data Flow
- Technical Support Data Flow

Data Protection by Design and by Default

Data Protection by Design or Privacy by Design is the practice of proactively implementing data protection in your systems and your processes. We believe that the best way to protect the data is to practice data protection in our day to day processes and build it in our systems from the start instead of retroactively and reactively solving data privacy issues as a result of breach.

From the point of initiating the conversations with our customers, to building software, we believe that data protection needs to be the default and considerations need to be assessed and built from the earliest stage in processes that potentially impact data protection. Blue Marble Payroll practices Data Protection by Design from the very beginning and all the way through our processes.

- Data Protection Policy
- Policy
- Security Policy

Security and Data Breach Reporting

Timely reporting of data breaches to the appropriate subjects is important in mitigating the risks and fines associated with such an occurrence. Having a formal security and data privacy incident response plan is critical in making sure that customers, individuals, and Supervisory Authorities are aware of the impact. Blue Marble Payroll implements a formal incident response plan. Their policies speak to how data subjects are to be notified, and where appropriate, how to work with various supervisor authorities.

- Data Breach Procedure
- Security Response Plan

Data Protection Impact Assessments

Having impact assessments as part of an organization's process will help them to identify and understand the current and new risks in their systems and processing activities. Impact assessments will help by:

- identifying when projects involve the collection of data individuals
- Identify whether information about individuals will be disclosed
- Identify when new systems are introduced that may raise privacy and data protection issues
- Identify whether an individual's data raises issues or concerns

Blue Marble Payroll's commitment to Data Protection by Design includes the use of Data Protection Impact Assessments. Each new process and system implemented within the organization will first go the process to understand if a Data Protection Impact Assessment is needed, then secondly an Impact Assessment is implemented if a risk to data privacy is identified.

Maintain Compliance with Rights of Data Subjects

More and more, data privacy laws are focusing on the rights of the individual. These considerations need to be taken into account and processes and systems need to be built to support these rights. Getting explicit consent to store and transfer an individual's personal data, the right to be forgotten, the right to object, the right to have their data removed, and data retention periods are important rights that every organization needs to be able to support. Blue Marble Payroll has documented and practiced policies that speak to data retention and the rights of the data subjects.

- Consent Policy and Procedure
- Data Subject Requests and Rights Procedure

Vendor Management and Commitments to Confidentiality

We not only need to commit to data protection ourselves, but need to hold all parties involved in an individual personal data accountable for how they are handling confidentiality and data protection. Blue Marble Payroll works with their vendors and partners to have the processes and controls in place and to have the commitment to data protection.

- Data Protection Addendum
- EU-U.S. Privacy Shield Framework
- Third party System Inventory
- Third party SLA

Implementation of Appropriate Technical and Organization Protection Measures

Implementing appropriate technical and organization protection measures is essential in protecting data privacy. Regular testing of those controls will ensure the processes and systems are operating with data privacy and confidentiality in mind. Internal monitoring and audits along with working with outside cybersecurity experts to audit the systems are important aspects of this. SSAE18 (SOC1/SOC2) testing and ISO 27001 certification are steps you can take to make sure your organization is maintaining compliance. Blue Marble Payroll is working with a third-party firm in demonstrating how they achieve key compliance controls and objectives through SSAE18 (SOC1/SOC2).

- Internal / External Audits
- Backup Policy
- Data Protection Controls
- Disaster Recovery Plan
- SDLC and Change Management
- WebGlobe SLA

Data Protection Team

To help educate and implement compliance within the organization the designation of a data protection officer is needed. The role of this officer will be to understand the laws that govern data protection, educate and enforce data protection within the organization and with their customers, vendors and partners.

Blue Marble Payroll's data protection officer will lead a team of “champions” within the organization. Each business unit has a designated “champion” that helps implement data protection process within their respective unit.

Our data protection officer is also the public face to the data protection practices and issues the organization faces. They will be the contact to Supervisory Authorities and to customers in an unfortunate occurrence of a data or security breach.

Robert Brose CIO/DPO
rbrose@bluemarblepayroll.com
847-565-5709

For questions and queries on data protection policy, please send to DPO or privacy@bluemarblepayroll.com