BODET SOFTWARE

INFORMATION REGARDING THE IMPLEMENTATION OF GDPR

Bodet
Software

CONTENTS

INTRODUCTION: WHAT IS GDPR?

The **General Data Protection Regulation** - EU 2016/679 (GDPR) - was adopted in April 2016 and will be applicable from 25 May 2018. It replaces the European Data Protection Directive (95/46/EC), adopted at the end of 1995, which governs the protection of individuals with respect to personal data processing and the open circulation of this data. GDPR strengthens and unifies data protection for individuals residing in the European Union.

GDPR supplements the French Data Protection Law (78-17) of 6 January 1978 which regulates personal data processing rights and brings computer processing within a human rights framework.

"IT must serve each citizen. It must develop within the framework of international cooperation. It must not infringe upon human identity, human rights, privacy or individual and public freedoms." »

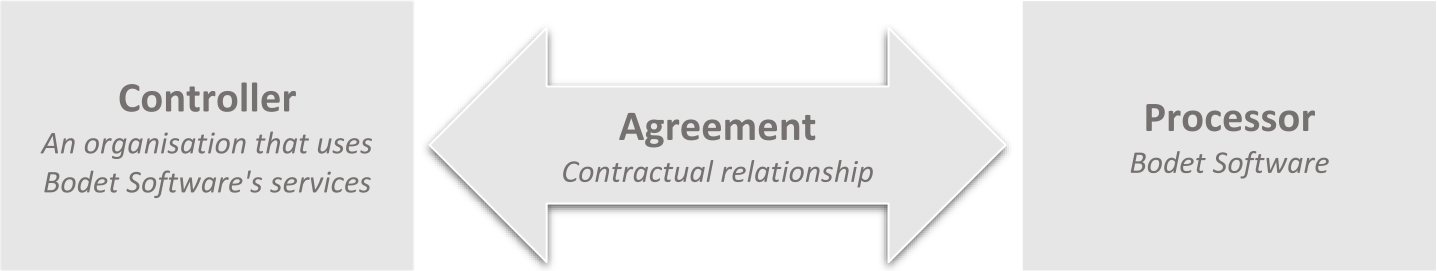
GDPR **applies to any organisation, whether based in the European Union (EU) or not, which processes the data of individuals residing in the European Union.** For example, the HR data of an intern who is a citizen of a country outside the EU and on a short internship in the European Union, is protected by this regulation.

Should an organisation breach obligations to protect personal data, the data protection authorities may, in addition to applying criminal **sanctions** (such as fines or imprisonment), take measures commensurate to the offence such as giving a warning or caution, placing a temporary or permanent restriction on a processing activity or enforcing an obligation to fulfil individuals' requests to exercise their rights (rectify, restrict or delete data). Fines may reach up to **4% of the company's global annual turnover or 20 million euros**.

RESPONSIBILITIES RELATED TO PERSONAL DATA PROCESSING

GDPR defines two separate roles:

- The **Controller**: an individual or legal entity that decides to implement a processing activity and defines its terms. *E.g. an HR director decides to set up attendance time monitoring using Bodet Software's Kelio software.*
- The **Processor**: an individual or legal entity to whom the processing activity defined by the Controller may be delegated. *E.g. Bodet Software maintains Kelio software.*



Controller
An organisation that uses Bodet Software's services

Agreement
Contractual relationship

Processor
Bodet Software

The Processor's responsibility towards the Controller is expressed as a **contract** between the two parties. This mutual contractual commitment avoids the following situations arising:

- A Controller attempting to transfer all its responsibilities for regulation to its Processor;
- A Processor refusing to bear any contractual responsibility.

The contract **establishes a chain of trust and clarifies the roles and responsibilities of each party.** Therefore Bodet Software proposes specific GDPR-related clauses to its clients, which are included in its contracts.

By hosting or maintaining its software, Bodet Software plays a Processor role, according to the definition of GDPR. This sub-contracted processing takes place within the framework of a contractual relationship with its clients, who remain responsible for the data processing that takes place and its controls.

Therefore the clients, described in this document as Controllers, must be able to receive the necessary guarantees and control the processing of their data through processes and solutions provided by Bodet Software. The rest of this document lists the responses to GDPR requirements that Bodet Software offers its clients. They are based on factors in place both before and after the regulation is adopted.

BODET SOFTWARE AS A PROCESSOR - RESPONSES TO GDPR COMPLIANCE

COMPLIANCE WITH LEGISLATION AND PRACTICE PRIOR TO THE IMPLEMENTATION OF GDPR

Aware of the inherently sensitive nature of data managed through its software products, Bodet Software has always been especially attentive in implementing measures to protect and manage this information. In addition to observing the relevant texts, for several years Bodet Software has taken proactive measures that reflect the requirements now regulated by GDPR.

- ***1997***: Bodet Software's ISO 9001 certification
- ***1998***: Creation of an independent testing department separate from the software design teams
- ***2001***: Installation of Bodet Software employees on dedicated and completely secure premises
- ***2004***: ISO 14001 certification
- ***2012***: Appointment of a Quality Engineer dedicated to software design
- ***2015***: Provision of a SaaS offering with an ISO27001 certified hosting solution
- ***2016***: Appointment of a Security Engineer dedicated to software design
- ***2017***: Since 2017: Annual software security audits, led by independent experts
- ***2018***: Dedicated software DPO appointed

RESPONSES FOLLOWING REQUIREMENTS INTRODUCED BY GDPR

The GDPR expresses new requirements to which Bodet Software has adapted its responses:

Requirement	Clarification of the Controller's responsibilities	Bodet Software's responses as a Processor
Accountability and appointment of a DPO	Organisations are accountable for the personal data they manage. GDPR imposes a duty to prove that data is properly managed and protected. To do so, organisations must put in place: ○ a documented internal policy of this data management ○ 3 records (processing activities, categories of processing and breaches) ○ A data map and an impact analysis, as well as an action plan known as a Privacy Impact Assessment (PIA) The burden of proof is placed on companies, whether they manage their data themselves or delegate its processing to Processors. They are therefore responsible for inspecting their Processors (article 26). To simplify inspection and compliance procedures, companies must appoint a **single point of contact** or a DPO (**Data Protection Officer**) (Article 37). The DPO is a contact who specialises in personal data protection. They are in charge of maintaining privacy and applying the data protection rules. They are also a special contact for everyone involved in personal data collection or processing as well as the supervisory authority.	**Appointment of a DPO** (Data Protection Officer) in charge of managing private data for Bodet Software and a single point of contact for its clients. The DPO is in charge of setting up a steering committee and a private data management system and monitoring an action plan specific to Bodet Software. The DPO has been declared to CNIL, the supervisory authority in France which is the equivalent body to the Information Commissioner's Office (ICO) in the UK.
Joint accountability	In the past, the controller was solely accountable towards the authorities. Now, processors are also accountable and there is a duty of mutual assistance. The aim is to create a chain of trust in data processing.	**Contracts and new amendments** between Bodet Software and its clients now include specific clauses, dedicated to the protection of personal data.
Privacy by default	The controller must ensure that personal data is protected by guaranteeing a maximum level of protection	Bodet Software has implemented **security measures**: - Information System security policy - Buildings monitored and protected by access control - Secure servers and backed up data - Information system audited regularly

		Bodet Software has chosen **highly secure hosting centres**: - ISO27001 certifications - highly secure firewalls - backup redundancy - high availability servers
		Bodet Software strictly ensures that **it follows secure processes**: - regular security audits by independent security experts - encryption of data transferred (HTTPS, VPN) - protection by authentication * - default rights restricted - database backup procedures - data retention times, with pre-set purges based on the French supervisory authority’s (CNIL) recommendations which is the equivalent body to the Information Commissioner’s Office (ICO) in the UK. A **dedicated Quality Engineer** and **Security Engineer**, who are part of the design team, ensure these measures are taken.
Privacy by design	Privacy by Design consists in taking into account rights and obligations concerning personal data when a processing activity is created or modified and taking proactive and preventive measures to prevent any incidents relating to privacy infringement. This notion specifies the right to consent (opt-in), rectify, be forgotten or data portability.	Bodet Software employees are informed about data protection.
		Bodet Software developers are **informed** about security and software code is analysed by **automatic analysis tools** to ensure best practice is observed (OWASP). The **required data fields** in Kelio software are **kept to the strict minimum** necessary for each process to run.
Right to be forgotten	Any request to delete data concerning individuals is the responsibility of the controller. It must be fulfilled free of charge and within 30 days.	**Software administrators may delete** all or some data related to an individual. Technical records are deleted over time or through a request to the Bodet Software support department.

Right to consult/correct **Data portability**	Any request to consult and correct data concerning individuals is the responsibility of the controller. A person must also be able to retrieve the data they have provided in a re-usable format and transfer it to a third party. The response must be provided free of charge within 30 days.	**Access and correction rights can be configured** by software administrators via a dedicated module. Bodet Software's products offer **integrated reporting and data export solutions** in standard formats (PDF, XLSX, CSV), enabling the retrieval of this data. These solutions are in the hands of software administrators.
Consent (opt-in)	As a controller, the client is in charge of ensuring that its employees have opted in to the use of their personal data.	To avoid optional data being input without people's consent, the configuration of Kelio users' profiles enables them to prohibit optional data from being entered.
Data transfer outside the EU	A data controller must guarantee that GDPR is applied across the entire processing chain, even for processes outside the EU which require additional measures (exemptions, declarations, binding corporate rules, individual and explicit consent, etc.)	Bodet Software **does not transfer its clients' data outside the European Union.**
Processing records and impact analysis (Privacy Impact Assessment / PIA)	The controller must keep an up-to-date **record** (art. 30.a) of the personal data it processes. This record is a map of its data-flow which must also be linked to an impact analysis **Privacy Impact Assessment** (PIA) to assess the risks to data protection and potentially take mitigating action.	For each solution it markets, Bodet Software offers a **pre-populated processing record template**. Clients may revise it themselves, adapt it to their purposes and incorporate it into their company's processing record.
Record of all categories of processing activities	Any company that processes personal data must also keep an up-to-date list of its own processing partners with their respective single points of contact (art.30.b)	Bodet Software's GDPR **single point of contact** for the supervisory authority is dpo@bodet-software.com
Notifications	The controller must report a data breach to its supervisory authority (Information Commissioner's Office (ICO) in the UK) as soon as possible (within 72 hours). The people concerned must be informed if this breach is likely to put their rights and freedoms at high risk. Any breaches must be listed in a dedicated record.	If Bodet Software is alerted to a personal data breach, the company will send notification to the client's single point of contact or DPO **within a maximum period of 48 hours** after acknowledging it.

**Passwords and biometrics*

User passwords are not stored, only a hash of the password is stored. When verifying authentication, the hash is recalculated and compared to the hash stored in the database. The password cannot be deduced from the hash.

Biometric data is sensitive personal data. The Kelio software solution does not store biometric fingerprints. When a biometric record is made, the fingerprint is analysed to extract the specific characteristics, which are encrypted in a non-reversible digital format. This result serves as a reference. In a biometric verification (e.g. badge), the captured fingerprint is processed in the same way and the mathematical result is compared with the reference value. Thus, whether you use a centralized enrollment on the server, an enrollment specific to each terminal or an enrollment on a secure badge, the fingerprint itself is neither stored nor retrievable.

ACTIONS IMPLEMENTED BY BODET SOFTWARE

Bodet Software's commitment is part of an ongoing approach to quality, the environment, security and personal data protection and involves various measures such as:

A DEDICATED TEAM

Bodet Software has appointed a data protection officer (DPO) who carries out their duties for the company as a software publisher, SaaS (Software as a Service) solution provider, software integrator and provider of software support services. The DPO has set up a dedicated team in charge of ensuring the GDPR’s requirements are met. It comprises the following people:

- Managing Director
- Client Support Manager
- SaaS Administration Manager
- Information Systems Manager
- Marketing and Communications Manager
- Software Design Office Manager
- Data Protection Officer (DPO)

COMPANY MEASURES

- ISO9001 and ISO14001 certification
- Implementation and control of a Personal Data Management Policy via a dedicated management system that aims to achieve a high level of compliance via the ongoing improvement of its processes.
- Monitoring and protection of premises against any physical intrusion and restricted access control for sensitive physical areas
- Monitoring and protection of the Information System against any digital attack.
- Information System security policy (updates, activity audits, anti-virus, anti-spam and password management policy)
- Regular audit of the Information System by independent experts
- Back-up of company data
- Raising staff awareness about the security and protection of personal data
- Online collection: networks protected by standard systems (HTTPS, firewalls and authentication)
- No data transferred outside the EU
- GDPR compliance audits by an independent body and acknowledgement of comments made in the company's general policy
- Revision of contracts to take into account GDPR compliance

SOFTWARE MEASURES

Bodet Software has created innovative and adapted software solutions for more than 30 years. This software incorporates intrinsic security solutions such as:

- Data transfer encryption (HTTPS and VPN)
- Native authentication (with a dedicated password management policy) or authentication interfacing with your own directories (LDAP, SAML, CAS, etc.)
- A limited and configurable length of time for client sessions
- Access rights that are restricted by default and configurable
- Login and functional and technical data (logs) modification traceability solutions
- Data retention times adapted to the different possible processes that can be customised by your administrators

We are leading an awareness and ongoing quality and security improvement policy with our research and development staff. This policy is strengthened by a dedicated quality engineer and security engineer as well as by continuous integration and automatic code analysis tools following security best practice (OWASP). Furthermore, we regularly use independent security experts to audit our software.

HOSTING MEASURES (ONDEMAND SOLUTION)

- We choose the hosting centres that we use carefully. Our hosting centres are certified for their security procedures (ISO27001) and located in countries that are considered to be reliable for data protection (France and Switzerland).
  Access to the servers hosted is protected and filtered (anti-virus, anti-spyware, intrusion prevention) and can be filtered by inbound IP (restriction by source IP). Furthermore, all the measures are taken to guarantee the high availability of our software solutions (data back-up and restoration, data centre replication).

- Data is transferred via secure protocols (HTTPS and VPN) and our clients have the possibility of testing our solutions in a test environment, and if the contract ends, data is returned to our clients before destruction.

- Operations relating to hosted software solutions are carried out by a restricted and dedicated team.

HOW TO CONTACT US

If you have any questions or complaints or if you would like to make recommendations or comments to improve the quality of Bodet Software's services, you can contact our client support via this link https://bsupport.bodet-software.com, or send our DPO an email (dpo@bodet-software.com) or contact us by post at the following address:

BODET SOFTWARE S. A. S.
Boulevard du Cormier
CS 40211
49302 CHOLET CEDEX