GDPR Compliance

BPM'ONLINE COMPLIANCE WITH GDPR REQUIREMENTS

bpm'online

Table of Contents

Introduction

European Union's General Data Protection Regulation 2016/679 (GDPR) comes into force May 25, 2018 and replaces the Data Protection Directive 95/46/EC. In short, the GDPR is a set of regulations that ensure appropriate protection of personal data of EU-based individuals. Unlike its predecessor, the GDPR contains strict regulations on the implementation of safeguards and compliance with its provisions. The GDPR affects both the EU companies and companies that process or store information of EU residents.

Bpm'online vision is to help companies ACCELERATE deployment and transformation, which we achieve through providing a unique synergy of low-code platform for business process management and CRM, with extensive marketplace of apps and templates. Customer success in ensuring security, transparency and full compliance with legislative norms is a top priority whenever we develop our products and services. This includes GDPR compliance, ISO/IEC 27001:2013 certification and much more. For more information, see our official statement on GDPR implementation.

This document is aimed at informing bpm'online customers and partners about compliance of bpm'online (company, software and service) with the GDPR requirements. The first part of the document covers implementation of compliance with GDPR articles in bpm'online and its customers. The second part of the document contains description of GDPR-related procedures in bpm'online software and links to the User Guide articles that cover related functions in detail.

Compliance insights and perspectives

It is very important to remember that GDPR contains requirements to the processing of personal data by data processors and data controllers. Software tools are only a part of the information processing workflow – along with internal policies and processes. Therefore, complete compliance with GDPR requirements implies more than just compliance of the software used for gathering, storing and processing personal data.

We have analyzed requirements contained in each GDPR article and provided insights and commentary on all articles that affect bpm'online. Compliance comments for each applicable article are broken down into three perspectives:

- Compliance of Bpm'online, Inc. as data processor – Bpm'online collects and processes personal data of thousands of customers, users and partners. In order to ensure our compliance with GDPR, we have all the processes and tools in place. Here we provide detailed insights on how we ensure compliance with GDPR articles as personal data processor.
- Compliance of Bpm'online, Inc. as controller – Bpm'online is CRM software, which is engaged in collecting and processing personal data. As its developer, Bpm'online, Inc. in one way or another determines the purposes and means of processing personal data. This perspective covers features of bpm'online software that ensure its readiness to process personal data according to GDPR or tools that you can use to ensure your company's compliance with the GDPR requirements. This perspective also covers any measures that Bpm'online has taken to ensure the compliance of its services (bpm'online cloud or "SaaS") with GDPR requirements.
- Compliance of your organization as processor – Most GDPR requirements cannot be met simply by using tools and features available in your CRM software. Several GDPR articles require that you audit your current policies or adopt additional policies and regulations within your company. This perspective will give you insights as to which organizational changes within your company are required to ensure compliance with GDPR. Additionally, since bpm'online on-site users have complete control over bpm'online servers and database, additional steps may be required (steps that have been taken care of by Bpm'online, Inc. for bpm'online cloud) to ensure compliance with GDPR.

We did not comment on the articles that do not affect compliance of Bpm'online, Inc. and its customers as data processors, or Bpm'online, Inc. as controller.

Glossary and definitions

In addition to definitions stipulated in Article 4, this document uses the following terms, specific to bpm'online business:

Bpm'online, Inc. – bpm'online company, acting as a processor and/or controller of personal data of its customers, business and marketing contacts.

Bpm'online software – bpm'online application of the latest released version, regardless of deployment option (cloud or on-site), product configuration (sales, marketing, service, etc.).

Bpm'online cloud – bpm'online software, hosted on the premises of Bpm'online, Inc. (the cloud deployment option, “SaaS”).

Bpm'online on-site – bpm'online software, hosted on the premises of bpm'online customers (the on-site deployment option).

Bpm'online customers – any company or individual who has an active license of bpm'online software, is using it in their business and acts as a processor and/or controller of personal data of their own customers.

Bpm'online sections that contain personal data – modules within bpm'online software, including, but not limited to: Contacts, Documents, Invoices, Agreements, Leads and Application forms sections.

Transparent information, communication and modalities for the exercise of the rights of the data subject

See Article 12

Compliance of Bpm'online, Inc. as processor

As part of GDPR implementation, Bpm'online, Inc. assigns a data protection officer (DPO) and provides individuals with means of contacting the DPO (via a web form at bpmonline.com or by direct email address). The data protection officer processes and replies to the requests from individuals to correct, remove or block their personal data from processing.

Compliance of Bpm'online, Inc. as controller

Bpm'online software features	Bpm'online software has all tools necessary for the DPO to perform their duties. Global search – Find all bpm'online records that contain personal data throughout the bpm'online database. Deletion function – You can easily delete records that contain personal data, as well as their connected records. Change log – Logs all operations (including deletion) with bpm'online records (including records with personal data). For more information, see: ● Verification of the requestor upon personal data inquiry ● Quick selection of all contacts or any other records that are subject to the GDPR ● Providing a copy of the customer's personal data upon request ● Deleting individual's personal data
Additional tools	GDPR compliance toolkit (available free of charge at bpm'online marketplace) enhances bpm'online software with tools needed to implement personal data anonymization/erasing policies.

Compliance of your organization as data processor

Internal policies and regulations	Appoint data protection officer – Bpm'online customers must ensure their compliance as personal data processors by assigning a data protection officer role, implementing means of contacting the DPO by data subjects, controllers and supervisory authorities and providing the DPO access to the corresponding features in bpm'online software. Set up the audit log and change log – Bpm'online customers must set up change log in bpm'online software.
Additional measures for bpm'online on-site	Set up logging on the DBMS level – Set up the DBMS event audit to track any operations with the database that did not originate from the application server (running database scripts, etc.).

Information to be made available or given to the data subject

See Article 13

Compliance of Bpm'online, Inc. as processor

Information that must be made available or given to the data subject is publicly available at bpmonline.com in the form of "Privacy policy" statement, which can be accessed by the data subjects from any web form that collects personal data (landing pages, trial registration pages, etc.). Additional information is provided upon request from the data subject.

Compliance of Bpm'online, Inc. as controller

Bpm'online software features	Bpm'online software has all tools necessary for making the required information available to the data subjects. Storage and access – All personal data stored in bpm'online software is available for your organization's Data Protection Officer (DPO) and your other employees, who are responsible for handling such customer requests – as long as they are bpm'online users. Information portability – Utilizing the default bpm'online software tools (copy, export and other functions), your employees can further use this information to fulfill requests from the data subjects. Business processes and automation – You also have out-of-the-box bpm'online tools that enable you to design and run business process that will send out this data to the customer (i.e., via email) upon a request from the DPO or user. Customer portal – If your bpm'online software has the "customer portal" function, you can publish information listed in Article 13 as a knowledge base article available to the portal users.
Additional tools	GDPR compliance toolkit (available free of charge at bpm'online marketplace) adds the "GDPR insights" report that will provide the Data Protection officer with complete report on personal data of a particular contact.

Compliance of your organization as data processor

Internal policies and regulations	Implement (or review) publicly available privacy statement – Your privacy notice must contain information listed in GDPR Article 13 (1,2). Make sure the privacy notice is read and understood by your customers – Make sure that your privacy statement is displayed whenever personal data of your customers is collected, as well as whenever you inform the customers that their personal data will not be collected. Make sure that your privacy statement delivers information "in a concise, transparent, intelligible and easily accessible form, using clear and plain language".
Additional measures for bpm'online on-site	No additional measures needed

Information to be provided where personal data have not been obtained from the data subject

See Article 14

Compliance of Bpm'online, Inc. as processor

Bpm'online, Inc. only collects personal data directly from the data subjects, using web forms completed by the data subjects, incoming emails from the data subjects, etc. Any practices that involve “indirect” collection of personal data, such as purchasing databases of marketing contacts, are not endorsed by Bpm'online, Inc.

Compliance of Bpm'online, Inc. as controller

Bpm'online software features	By default, all personal data is obtained by bpm'online from the data subjects directly (using web forms, emails, etc.). Any exceptions to this will have to do directly with the specifics of your business (i.e., you obtain personal data from your partners). Compliance of contact data enrichment – bpm'online software has a “data enrichment” function, which uses personal data from the signatures in emails received from the data subjects. Since the data subject intentionally sends emails to your mailbox, it is safe to assume that any personal data in these emails is obtained directly from the data subject and Article 14, therefore, does not apply.

Compliance of your organization as data processor

Internal policies and regulations	Review all sources where your organization obtains personal data from – if you obtain any data from sources other than the data subjects themselves (i.e., you obtain personal data of your partner customers, of your customer’s employees), make sure that you provide the data subjects with details listed in Article 14. Implement (or review) publicly available privacy statement – If you do not directly collect personal data from the data subjects, your privacy notice must contain information listed in GDPR Article 14. Make sure the privacy notice is read and understood by your customers – Make sure that your privacy statement is displayed to the individuals whose personal data you collect. Make sure that your privacy statement delivers information “in a concise, transparent, intelligible and easily accessible form, using clear and plain language”.
Additional measures for bpm'online on-site	No additional measures needed

Right to access by the data subject

See Article 15

Compliance of Bpm'online, Inc. as processor

As part of GDPR implementation, Bpm'online, Inc. assigns a data protection officer (DPO) and provides individuals with means of contacting the DPO (via a web form at bpmonline.com or by direct email address). Upon request from the data subject, the data protection officer verifies their identity and provides the data subject with an electronic copy of their personal data.

Compliance of Bpm'online, Inc. as controller

Bpm'online software features	Bpm'online software has all tools necessary for the DPO to verify the identity of the data subject and provide them with a copy of their personal data. Global search and filters – Use global search and filter features available in bpm'online software to find all records that contain personal data of a particular individual throughout the bpm'online database. Exporting list data – Use data export feature to create a portable copy of personal data (in Excel format) for sending it to the individual. MS Word report templates – Use the MS Word printable feature to create a template for exporting a portable copy of personal data (in Word or PDF format) for sending it to the individual. Attachments and notes – Download attachments that contain personal data for sending them to the individual. For more information, see: ● Set up data protection officer working environment ● Verification of the requestor upon personal data inquiry ● Providing a copy of the individual's personal data upon request
Additional tools	GDPR compliance toolkit (available free of charge at bpm'online marketplace) enhances bpm'online software with tools needed to implement personal data anonymization/erasing policies. With the GDPR compliance toolkit, a user can generate the "GDPR insights" report on a contact level that includes all the personal data from customer profile (the report can be customized and expanded with additional fields and details, if needed).

Compliance of your organization as data processor

Internal policies and regulations	Appoint data protection officer – Bpm'online customers must ensure their compliance as personal data processors by assigning a DPO role in their organizations. Set up DPO workplace in bpm'online and grant the DPO role all permissions necessary to perform their duties. Provide the individuals with means of contacting your DPO (by phone, email, web form, etc.).
Additional measures for bpm'online on-site	No additional measures needed

Right to rectification or erasure of personal data and restriction of processing

See: Article 16, Article 17, Article 18, Article 19

Compliance of Bpm'online, Inc. as processor

As part of GDPR implementation, Bpm'online, Inc. assigns a data protection officer (DPO) and provides individuals with means of contacting the DPO (via a web form at bpmonline.com or by direct email address). Upon request from the data subject, the data protection officer verifies their identity and corrects, removes or blocks their personal data from processing.

Compliance of Bpm'online, Inc. as controller

Bpm'online software features	Bpm'online software has all tools necessary for the DPO to verify the identity of the data subject and correct remove or block their personal data from processing. Global search and filters – Use global search and filter features available in bpm'online software to find all records that contain personal data of a particular individual throughout the bpm'online database. Edit records – You can modify records that contain personal data to rectify them. Deletion function – You can easily delete records that contain personal data, as well as their connected records. Record permissions – You can restrict access to the records that contain personal data, so that they are removed from processing. Change log – This bpm'online software feature logs all operations (including deletion) with bpm'online records (including records with personal data). Use the change log to provide the proof of rectification, erasure or restriction from processing of personal data. For more information, see: • Set up data protection officer working environment • Verification of the requestor upon personal data inquiry • Quick selection of all contacts or any other records that are subject to the GDPR • Deleting individual's personal data • Restricting customer's personal data processing • Set up the audit log and change log
Additional tools	GDPR compliance toolkit (available free of charge at bpm'online marketplace) enhances bpm'online software with tools needed to implement personal data anonymization/erasing policies.

Compliance of your organization as data processor

Internal policies and regulations	Appoint data protection officer – Bpm'online customers must ensure their compliance as personal data processors by assigning a DPO role in their organizations.

	Set up DPO workplace in bpm'online and grant the DPO role all permissions necessary to perform their duties. Provide the individuals with means of contacting your DPO (by phone, email, web form, etc.). Set up the audit log and change log – Bpm'online customers must set up change log in bpm'online software to be able to prove the modification or erasure of personal data.
Additional measures for bpm'online on-site	Set up logging on the DBMS level – Set up the DBMS event audit to track any operations with the database that did not originate from the application server (running database scripts, etc.).

Right to data portability

See Article 20

Compliance of Bpm'online, Inc. as processor

As part of GDPR implementation, Bpm'online, Inc. assigns a data protection officer and provides individuals with means of contacting the data protection officer (via a web form at bpmonline.com or by direct email address). The data protection officer provides the data subjects with a copy of their personal data upon request.

Compliance of Bpm'online, Inc. as controller

Bpm'online software features	Bpm'online software has all tools necessary for the DPO to verify the identity of the data subject and provide them with a copy of their personal data. Global search and filters – Use global search and filter features available in bpm'online software to find all records that contain personal data of a particular individual throughout the bpm'online database. Exporting list data – Use data export feature to create a portable copy of personal data (in Excel format) for sending it to the individual. MS Word report templates – Use the MS Word printable feature to create a template for exporting a portable copy of personal data (in Word or PDF format) for sending it to the individual. Attachments and notes – Download attachments that contain personal data for sending them to the individual. For more information, see: ● Set up data protection officer working environment ● Verification of the requestor upon personal data inquiry ● Providing a copy of the individual's personal data upon request
Additional tools	GDPR compliance toolkit (available free of charge at bpm'online marketplace) enhances bpm'online software with tools needed to implement personal data anonymization/erasing policies. With the GDPR compliance toolkit, a user can generate the "GDPR insights" report on a contact level that includes all the personal data from customer profile (the report can be customized and expanded with additional fields and details, if needed).

Compliance of your organization as data processor

Internal policies and regulations	Appoint data protection officer – Bpm'online customers must ensure their compliance as personal data processors by assigning a DPO role in their organizations. Set up DPO workplace in bpm'online and grant the DPO role all permissions necessary to perform their duties. Provide the individuals with means of contacting your DPO (by phone, email, web form, etc.).
Additional measures for bpm'online on-site	No additional measures needed

Responsibility of the controller

See Article 24

Compliance of Bpm'online, Inc. as controller

Bpm'online cloud (SaaS)	As part of ISO/IEC 27001:2013 compliance, Bpm'online, Inc. regularly reviews information security policies. This confirms that all technical and organizational measures have been taken to ensure compliance of bpm'online cloud (SaaS) with GDPR requirements. Applicable ISO controls (Bpm'online compliance is confirmed with "The applicability of regulation" statement, v.1.2, 4/4/2017): ● A.5.1.2 Review of the policies for information security. ● A.6 Organization of information security.

Compliance of your organization as data processor

Internal policies and regulations	N/A (you are all set!)
Additional measures for bpm'online on-site	Establish information security policies and regulations – Audit your information security system, establish or review data security policies. You can demonstrate compliance with GDPR Article 19 by obtaining and renewing corresponding certificate, such as ISO. Implement corresponding data protection policies and be ready to demonstrate it.

Data protection by design and by default

See Article 25

Compliance of Bpm'online, Inc. as processor

As part of ISO/IEC 27001:2013 compliance, Bpm'online, Inc. regularly audits internal information security risks. Bpm'online has also implemented data-protection principles, such as pseudonymisation.

Applicable ISO controls (Bpm'online compliance is confirmed with "The applicability of regulation" statement, v.1.2, 4/4/2017):

- A.12.7 Information systems audit considerations.
- A.18.2 Information security reviews.

Compliance of Bpm'online, Inc. as controller

Bpm'online software features	Organizational roles – Create organizational roles of users who will be working with personal data. Object permissions – Assign access permissions in sections that contain personal data. Restrict users and roles from viewing any personal data that is not processed by them. Grand users and roles who are engaged in processing personal data minimum access permissions needed for processing personal data (i.e., restrict view access to columns whose data is not used for processing, etc). Landing pages and web forms – Review your landing pages and web forms, as well as information that bpm'online gathers from each web form (the list of fields populated in bpm'online records after an individual submits a web form) and remove any fields that are not used in your company processes.
Additional tools	GDPR compliance toolkit (available free of charge at bpm'online marketplace) enhances bpm'online software with tools needed to implement personal data pseudonymisation/minimization policies.
Bpm'online cloud (SaaS)	As part of ISO/IEC 27001:2013 compliance, Bpm'online, Inc. regularly audits information security risks to the bpm'online SaaS. Applicable ISO controls (Bpm'online compliance is confirmed with "The applicability of regulation" statement, v.1.2, 4/4/2017): ● A.12.7 Information systems audit considerations. ● A.18.2 Information security reviews.

Compliance of your organization as data processor

Internal policies and regulations	Audit your information security risks - Perform an internal audit of risks to your information security.
Additional measures for bpm'online on-site	No additional measures needed

Joint controllers

See Article 26

Compliance of Bpm'online, Inc. as controller

Bpm'online cloud (SaaS)	Upon request, Bpm'online can determine responsibilities with any other controller who, according to Article 26, acts as a “joint controller” with Bpm'online.

Compliance of your organization as data processor

Internal policies and regulations	N/A (you are all set!)
Additional measures for bpm'online on-site	Identify companies that may act as joint controllers towards you and agree upon your mutual responsibilities: exercising of the rights of the data subject and your respective duties to provide the information (Article 13, 14) and a contact point.

Processing under the authority of the controller or processor

See Article 29

Compliance of Bpm'online, Inc. as processor

According to internal policies and regulations of the Bpm'online, Inc, the personal data are stored and processed according to the license agreement with bpm'online users or consent of the data subject whose personal data is provided to bpm'online.

Compliance of Bpm'online, Inc. as controller

Bpm'online software features	Attachments and notes – use this detail in the Contacts section of bpm'online to attach license agreement according to which your customers and other individuals give you consent for processing of their personal data.
Additional tools	GDPR compliance toolkit (available free of charge at bpm'online marketplace) enhances bpm'online software with tools needed to implement personal data anonymization/minimization policies.
Bpm'online cloud (SaaS)	Your license agreement with Bpm'online, Inc. – Bpm'online, Inc. processes personal data of your customers and other individuals that you enter in bpm'online software on your behalf. You give your consent to this processing in your license agreement with Bpm'online, Inc.

Compliance of your organization as data processor

Internal policies and regulations	Obtain consent from any other processors or controllers if you process personal data under their authority.
Additional measures for bpm'online on-site	No additional measures needed

Records of processing activities

See Article 30

Compliance of Bpm'online, Inc. as processor

Bpm'online, Inc. maintains records of processing the personal data under its responsibility (personal data in the internal CRM system of Bpm'online, Inc.).

Compliance of Bpm'online, Inc. as controller

Bpm'online software features	Use the Section wizard to add information that must be recorded – Add the columns for storing additional information about individuals and their personal data, as required by Article 30(1, 2). Set up audit log – The audit log records all system events, such as events related to user roles modification, access rights distribution, system settings value change and users' authorization in bpm'online. Set up change log – The change log records all operations (including deletion) with bpm'online records (including records with personal data). For more information, see: ● Add a required "Source of personal data" column to all sections that contain personal data ● Set up the audit log and change log ● Demonstrating the GDPR compliance to the Data Protection Authority
Additional tools	GDPR compliance toolkit (available free of charge at bpm'online marketplace) adds the "GDPR insights" report on a contact level that includes all the personal data from customer profile (could be extended manually with custom fields and details, if needed).
Bpm'online cloud (SaaS)	Your license agreement with Bpm'online, Inc. – As part of bpm'online SaaS, Bpm'online, Inc. logs operations with the customer databases and can provide logs of customer databases upon request from these customers.

Compliance of your organization as data processor

Internal policies and regulations	Make sure that you enable bpm'online functions for logging your processing activities by enabling the audit log and change log.
Additional measures for bpm'online on-site	Set up logging on the DBMS level – Set up the DBMS event audit to keep record of any operations with the database that did not originate from the application server (running database scripts, etc.).

Cooperation with the supervisory authority

See Article 31

Compliance of Bpm'online, Inc. as processor

Bpm'online, Inc. shall cooperate, on request, with the supervisory authority in the performance of its tasks. The extent of cooperation is determined by the request itself and GDPR regulations that apply in each particular case.

Compliance of Bpm'online, Inc. as controller

Bpm'online software features	Bpm'online software has a wide range of features and tools that can be used to demonstrate compliance with GDPR requirements upon request from the supervisory authority. Set up audit log – The audit log records all system events, such as events related to user roles modification, access rights distribution, system settings value change and users' authorization in bpm'online. Set up change log – The change log records all operations (including deletion) with bpm'online records (including records with personal data). Attachments and notes – Use the [Attachments] detail of the contact records of the data subjects for storing scan copies of agreements and demonstrating them upon request from the supervisory authority.
Bpm'online cloud (SaaS)	DBMS-level log – Contact bpm'online support and request DBMS log for demonstrating logs from the DBMS-level (SQL Server / Oracle Database) audit subsystem.

Compliance of your organization as data processor

Internal policies and regulations	Upon request from the Data Protection Authority, the Data Protection Officer must demonstrate compliance with the GDPR requirements. For more information, see: ● Add a required "Source of personal data" column to all sections that contain personal data ● Set up the audit log and change log ● Demonstrating the GDPR compliance to the Data Protection Authority
Additional measures for bpm'online on-site	Set up logging on the DBMS level – Set up the DBMS event audit to track any operations with the database that did not originate from the application server (running database scripts, etc.). DBMS-level log – Set up logging on the database level to be able to demonstrate logs from the DBMS (SQL Server / Oracle Database) audit subsystem.

Security of processing

See Article 32

Compliance of Bpm'online, Inc. as processor

As part of ISO/IEC 27001:2013 compliance, Bpm'online, Inc. implements technical and organizational measures for information security, including protection of personal data.

Applicable ISO controls (Bpm'online compliance is confirmed with "The applicability of regulation" statement, v.1.2, 4/4/2017) – all controls in the following sections:

- A.5 Information security policies.
- A.6 Organization of information security.
- A.7 Human resource security.
- A.8 Asset management.
- A.9 Access control.
- A.10 Cryptography.
- A.11 Physical and environmental security.
- A.12 Operation security.
- A.13 Communications security.
- A.14 System acquisition, development and maintenance.
- A.15 Supplier relationships.
- A.16 Information security incident management.
- A.17 Information security aspects of business continuity management.
- A.18 Compliance.

Compliance of Bpm'online, Inc. as controller

Bpm'online software features	Bpm'online software has access permission management system that you can use to fine-tune access permissions to personal data throughout the system. Bpm'online access permission management tools enable restriction of access to specific types of personal data (such as contact names, phone numbers, email addresses, etc.) for different users and user roles. Bpm'online customers can set up default access permissions that shall be applied to new personal data automatically. Organizational roles – Create organizational roles of users who will be working with personal data. Set up user and role structure in bpm'online software via the access permission management system. Object permissions – Assign access permissions in sections that contain personal data. Restrict users and roles from viewing any personal data that is not processed by them. Grant users and roles who are engaged in processing personal data minimum access permissions needed for its processing (i.e., restrict view access to columns whose data is not used for processing, etc.). Set up audit log – The audit log records all system events, such as events related to user roles modification, access rights distribution, system settings value change and users' authorization in bpm'online. Set up change log – The change log records all operations (including deletion) with bpm'online records (including records with personal data).

Additional tools	GDPR compliance toolkit (available free of charge at bpm'online marketplace) expands bpm'online software with tools required for compliance, such as pseudonymisation, and data minimization (Article 32 (1.)(a)).
Bpm'online cloud (SaaS)	Bpm'online cloud is compliant on the bpm'online side. Bpm'online SaaS is accessed via a secure connection. Personal data stored in bpm'online is encrypted on the database side. Bpm'online has pseudonymisation policies in place (when support staff is working with customer databases, for reporting purposes, etc.). Bpm'online internal processes are ISO/IEC 27001:2013 certified and comply with controls A.5-A.18 (as confirmed with "The applicability of regulation" statement, v.1.2, 4/4/2017).

Compliance of your organization as data processor

Internal policies and regulations	Set up a user and role structure and access rights to prevent unauthorized reading, copying, modification or deletion of personal data.
Additional measures for bpm'online on-site	Enable https – Set up secure connection protocol (https) to your bpm'online on-site application using verified SSL certificates. Use encryption tools on the DBMS level to secure the storage of your personal data.

Data protection impact assessment

See Article 35

Compliance of Bpm'online, Inc. as processor

As part of ISO/IEC 27001:2013 compliance, Bpm'online, Inc. regularly conducts information security impact assessments.

Applicable ISO controls (Bpm'online compliance is confirmed with "The applicability of regulation" statement, v.1.2, 4/4/2017):

- A.12.7 Information systems audit considerations.
- A.17.1.1 Planning information security continuity.
- A.18.2 Information security reviews.

Compliance of Bpm'online, Inc. as controller

Bpm'online cloud (SaaS)	Data protection risk assessments are regularly conducted by Bpm'online at the bpm'online cloud (SaaS) site (hosting, database, personnel, etc.) as part of ISO/IEC 27001:2013 compliance. Applicable ISO controls (Bpm'online compliance is confirmed with "The applicability of regulation" statement, v.1.2, 4/4/2017): ● A.12.7 Information systems audit considerations. ● A.17.1.1 Planning information security continuity. ● A.18.2 Information security reviews.

Compliance of your organization as data processor

Internal policies and regulations	Conduct data protection impact assessments on your side. Bpm'online data protection impact assessments can be used as part of your own assessments. We recommend that you communicate with Bpm'online information security officer.
Additional measures for bpm'online on-site	Users of bpm'online on-site will need to conduct deeper data protection impact assessments, including security of their website and DBMS, since Bpm'online data protection impact assessments cover bpm'online cloud site only. We recommend that you communicate with Bpm'online information security officer.

Prior consultation

See Article 36

Compliance of Bpm'online, Inc. as processor

As part of ISO/IEC 27001:2013 compliance, Bpm'online, Inc. regularly conducts information security impact assessments to identify information security risks (compliance with ISO controls A.12.7, A.17.1.1, A.18.2 is confirmed with "The applicability of regulation" statement, v.1.2, 4/4/2017).

Applicable ISO controls (Bpm'online compliance is confirmed with "The applicability of regulation" statement, v.1.2, 4/4/2017):

- A.12.7 Information systems audit considerations.
- A.17.1.1 Planning information security continuity.
- A.18.2 Information security reviews.

Bpm'online, Inc. has assigned a data protection officer (DPO) position. Bpm'online DPO shall conduct prior consultations if data protection impact assessments indicate that processing would result in a high risk in the future.

Compliance of Bpm'online, Inc. as controller

Bpm'online cloud (SaaS)	Bpm'online, Inc. data protection impact assessments do not indicate that processing would result in a "high risk". In addition, a number of risk mitigation measures has been implemented as a result of initial data protection impact assessments. No consultations under Article 36 are therefore required.

Compliance of your organization

Internal policies and regulations	If your organization acts as a data controller and if your data protection impact assessments indicate that processing would result in a high risk "in the absence of measures taken by the controller to mitigate the risk", you must contact your supervisory authority prior to processing. The supervisory authority is required to respond no later than within eight weeks (Article 36(2)).
Additional measures for bpm'online on-site	No additional measures needed

Data protection officer designation, position and tasks

See: Article 37, Article 38, Article 39

Compliance of Bpm'online, Inc. as processor

Bpm'online, Inc. has assigned a data protection officer (DPO) position. Bpm'online DPO has access to the tools and personal data referred to by Article 38. A special DPO feedback form has been implemented at bpmonline.com for contacting bpm'online DPO by individuals, controllers and supervisory authorities.

Compliance of Bpm'online, Inc. as controller

Bpm'online software features	Bpm'online software has all tools necessary for the DPO to perform their duties. Create a DPO workplace – bpm'online software has tools necessary to create a working environment for the data protection officer. Global search – Find all bpm'online records that contain personal data throughout the bpm'online database. Deletion function – You can easily delete records that contain personal data, as well as their connected records. Change log – The change log records all operations (including deletion) with bpm'online records (including records with personal data). For more information, see: ● Set up data protection officer working environment ● Verification of the requestor upon personal data inquiry ● Quick selection of all contacts or any other records that are subject to the GDPR ● Providing a copy of the customer's personal data upon request ● Deleting customer's personal data ● Restricting customer's personal data processing
Additional tools	GDPR compliance toolkit (available free of charge at bpm'online marketplace) adds the "GDPR insights" report on a contact level that includes all the personal data from customer profile (could be extended manually with custom fields and details, if needed).
Bpm'online cloud (SaaS)	Bpm'online DPO will not have access to the personal data stored on the bpm'online cloud premises and processed by your organization.

Compliance of your organization as data processor

Internal policies and regulations	Create a DPO position in your organization. Grant the DPO access to the tools and personal data referred to by Article 38. Implement means of contacting your DPO, for instance, publish DPO's direct email on your website or implement a feedback form for contacting the DPO by individuals, controllers and supervisory authorities.
Additional measures for bpm'online on-site	No additional measures needed

Right to lodge a complaint with a supervisory authority

See Article 77

Compliance of Bpm'online, Inc. as processor

Information about the right to lodge a complaint with a supervisory authority is publicly available at bpmonline.com.

Compliance of your organization as data processor

Internal policies and regulations	Inform the individuals whose personal data you process about their right to lodge a complaint with a supervisory authority. You can do this via your website, email, license agreement and other means.

GDPR compliance setup in bpm'online software

This chapter covers the general steps needed to prepare your bpm'online configuration for GDPR and instructions on how to use your bpm'online to assess and conduct day-to-day GDPR-related operations.

Set up data protection officer working environment

Prepare a working environment for the data protection officer (DPO). To do this in bpm'online:

1. Create a “Data Protection Officer” functional role.
2. Set up access rights for the “Data Protection Officer” role. Data protection officer (DPO) user must have access to all system sections that contain personal data (PD).
    a. Grant access to the following operations: “read”, “edit”, “delete”.
    b. Restrict access to adding new records (the “new” operation).

The list of default bpm'online sections that contain personal data (PD) is available in Reference section of this guide. Please note, that other bpm'online sections may also contain PD due to custom modifications made to your bpm'online software configuration.

3. Create a “Data Protection Office” workplace for the DPO.
4. Enable access to the “Data Protection Office” workplace for the “Data Protection Officer” role.
5. Add all sections containing personal data (PD) to the “Data Protection Office” workplace.

See also:

- How to add and set up functional roles
- How to give access to sections
- Workplaces setup
- The [Access to object] detail of the [Objects permissions] section

Set up the audit log and change log

Set up a log for the personal data stored in the system. To do this in bpm'online:

1. Set up the audit log to enable viewing the log of system operations.
2. Set up the change log to track changes made to system records.
3. Set up the DBMS event audit to track any operations with the database that did not originate from the application server (running database scripts, etc.).

See also:

- The [Audit log] section
- The [Change log] section
- SQL Server Audit (Database Engine)
- Oracle: Auditing Database Activity

Add a required “Source of personal data” column to all sections that contain personal data

Add the means to record the source of personal data in the system. To do this in bpm'online:

1. Open the Section Wizard for each section that contains personal data.
2. On the [Page setup] step, add a required lookup column “Source of personal data”.
3. Create lookup(s) “Personal data sources - <section name>”.
4. Fill in the lookups with possible sources of personal data in the corresponding section(s) (e.g., Excel list, website registration, etc.).

See also:

- Section wizard
- How to configure section pages

- The [Lookups] section

Bpm'online routine data protection procedures

Below are the recommended guidelines for day-to-day operations of your DPO in bpm'online.

Verification of the requestor upon personal data inquiry

DPO can quickly verify the identity of the requestor by comparing the information from the request with the information stored in bpm'online. To do this in bpm'online:

1. Run global search using the requestor's credentials.
2. Filter records in the corresponding section using the requestor's credentials via a standard or expanded filter.
3. Compare search results and request parameters.

See also:

- Global search
- Standard filter
- Advanced filter

Quick selection of all contacts or any other records that are subject to the GDPR

DPO can quickly select all contact records or records of any other type that are subject to the GDPR and view:

- Personal data
- Source of personal data
- Text of the subject's agreement to process their personal data
- Full log of activities related to the personal data (who performed the activity, when the activity was performed, which type of operation with the personal data was performed and how the operation concluded)

To do this in bpm'online:

1. Create a folder for quick access to the list of records.
2. Open the corresponding record page (such as the contact record page) to view:
    a. Personal data.
    b. Information about the source of the personal data.
    c. Copy of the personal data processing agreement
3. Open the [Change log] section to view information about changes made to personal data.

See also:

- How to create a folder
- Contact page
- The [View all changes in selected record] action in the [Change log] section

Providing a copy of the individual's personal data upon request (Right to data portability)

Based on a request from the personal data owner, DPO provides a copy of the customer's personal data (Right to data portability). To do this in bpm'online:

1. Run global search in bpm'online using the personal data owner's credentials.
2. Filter records in the corresponding section using the requestor's credentials via a standard or expanded filter.
3. Export search results.
4. Export attachments from the [Attachments] detail.

See also:

- Global search
- Standard filter
- Advanced filter
- Exporting list data
- How to work with attachments and notes

Deleting individual's personal data (Right to erasure)

Based on a request from the personal data owner, or when the personal data owner refuses the services of the data controller, DPO deletes personal data from bpm'online (Right to erasure). To do this in bpm'online:

1. Run global search in bpm'online using the personal data owner's credentials.
2. Filter records the corresponding section using the requestor's credentials via a standard or expanded filter.
3. Delete record(s) with the [Delete connected records] option selected.
4. The operation is logged in the bpm'online change log.

See also:

- Global search
- Standard filter
- Advanced filter
- How to delete records
- The [View all changes in selected record] action in the [Change log] section

Restricting customer's personal data processing (Right to restriction of processing)

Based on a request from the personal data owner, DPO restricts the ability to process personal data of the customer (Right to restriction of processing). To do this in bpm'online:

1. Run global search in bpm'online using the personal data owner's credentials.
2. Filter records in the corresponding section using the requestor's credentials via a standard or expanded filter.
3. Clear the contact's subscriptions to all bulk emails. This step is valid for bpm'online marketing and any custom configuration that contains the [Email] section.
4. Modify access right to record (restrict access to everyone except the DPO).

See also:

- Global search
- Standard filter
- Advanced filter
- How to manage subscriptions for various bulk email types
- Contact page, Communication options (bpm'online marketing)
- Access rights

Ensuring GDPR compliance in custom sections and standard sections that were customized to contain personal data

When creating a new custom section or customizing an existing section, check if the new (customized) section is subject to the GDPR. If this is the case:

- Grant access rights to "read", "edit", "delete" operation and restrict access to "new" operation for the "Data Protection Officer" user group.
- Add the new/modified section to the "Data Protection Office" workplace.
- Set up a folder for quick access to records that contain personal data.
- Enable logging changes in the section via the bpm'online change log.

Recommendations:

1. Create a dynamic folder for quick access to the records that contain personal data and are subject to the GDPR.
2. Set up a change log to enable tracking changes made to the system records. Make sure that you set up the log to monitor changes in all columns that contain personal data.

See also:

- The [Change log] section
- The [View all changes in selected record] action in the [Change log] section

Demonstrating the GDPR compliance to the Data Protection Authority

Upon request from the Data Protection Authority, the DPO must demonstrate compliance with the GDPR requirements.

To do this, demonstrate a “Digital footprint” of the operations with personal data. During the audit/confirmation of compliance with GDPR requirements, the following confirmations must be demonstrated:

- Confirmation of availability of certain categories of personal data (the categories will be specified as part of the request).
- Confirmation of erasure.
- Confirmation of amendments.
- Confirmation of personal data sources.
- Confirmation of personal data owners’ consent to process personal data (a scanned copy of agreement with the customer or a digitally signed agreement).
- Audit of system administrator and support staff activities (log of database level changes: scripts that create modify or delete data).

To do this in bpm'online:

1. Demonstrate records from bpm'online change log.
2. Demonstrate scan copies of agreements with the customers on the [Attachments] of the corresponding records.
3. Demonstrate logs from the DBMS-level (SQL Server / Oracle Database) audit subsystem.

See also:

- The [Change log] section
- The [View all changes in selected record] action in the [Change log] section
- SQL Server Audit (Database Engine)
- Oracle: Auditing Database Activity

FAQ

Can bpm'online ensure complete compliance of its customers with GDPR?

Bpm'online ensures compliance of its products and services with GDPR. However, a number of GDPR requirements refer specifically to the data processors (i.e. bpm'online customers) themselves and not to the tools used for gathering, storing and processing personal data. See Compliance insights and perspectives for details.

How do I enable data anonymization in bpm'online?

You can enable data anonymization by installing GDPR compliance toolkit (available free of charge at bpm'online marketplace), which enhances bpm'online software with tools needed to implement personal data anonymization/erasing policies.

How does bpm'online ensure my compliance with requirements regarding erasure of personal data?

Bpm'online, Inc. does not have access to the personal data stored in the databases of bpm'online customers. Bpm'online software has all tools necessary to ensure proper erasure of personal data, but the procedure itself can be initiated only by bpm'online customers. See Deleting individual's personal data (Right to erasure) for details.

Can bpm'online provide my customers with information regarding the processing of their personal data?

Bpm'online, Inc. does not have access to the personal data stored in the databases of bpm'online customers and therefore cannot verify whether specific personal data is stored or not. Bpm'online software has all tools necessary to verify the existence of specific personal data and obtain information that must be provided to the data owner. See Providing a copy of the individual's personal data upon request (Right to data portability) for details.

How does bpm'online record consent of my customers for processing of their personal data?

The specifics of obtaining consent for processing of personal data are different for different bpm'online customers. One way to record consent is to attach a scanned copy of agreement with the customer or a digitally signed agreement to the customer's profile. Bpm'online, Inc. does not have access to the personal data stored in the databases of bpm'online customers. See Demonstrating the GDPR compliance to the Data Protection Authority for details.

How does bpm'online ensure logging of operations with personal data (registration, obtaining consent for processing, modification, erasure, etc.)?

Bpm'online software records all operations with personal data, including adding, editing, deleting and accessing, through the change log and audit log. See Set up the audit log and change log for details.

Reference

Bpm'online default sections that contain personal data

No.	Section name	Fields with personal data	Possible sources	Notes
1	Contacts	Photo Full name Mobile phone Business phone Email Gender Home phone Skype Web Facebook Twitter Address City Country ZIP/Postal code Date of birth Employer Job title Department Full job title	Created manually Imported from an Excel file Saved on lead qualification Obtained during synchronization with Facebook Obtained during synchronization with Twitter Obtained during synchronization with Google Created when processing an incoming email Created automatically upon Single Sign-On authentication	GDPR Article 4 (1), All bpm'online products
2	Contracts	The [Attachments] detail is likely to contain files that are subject to the GDPR	Created manually	GDPR Article 4 (1) **Products:** sales enterprise, bank sales, bank customer journey, lending
3	Invoices	The [Attachments] detail is likely to contain files that are subject to the GDPR	Created manually	GDPR Article 4 (1) **Products**: sales commerce, sales enterprise
4	Documents	The [Attachments] detail is likely to contain files that are subject to the GDPR	Created manually	GDPR Article 4 (1) **Products**: sales team, sales commerce, sales enterprise, bank sales, bank customer journey, lending
5	Leads	Name Contact name Account name Mobile phone Email Web Job title Country	Created manually Imported from an Excel file Obtained from a web form on a landing page	GDPR Article 4 (1) **Products**: sales team, sales commerce, sales enterprise, marketing bank sales,

6	Application forms	Photo Contact name First name Middle name Last name Previous last name SSN Birth date Birthplace Gender Citizenship Social status Education (ID) Series (ID) Number (ID) Issued on (ID) Issued by Business phone Mobile phone Home phone Internal phone Other phone Skype Email Web Facebook Twitter Marital status Number of dependents Number of children Children under 14 years old (Spouse's) First name (Spouse's) Middle name (Spouse's) Last name (Spouse's) Birth date (Spouse's) Contact phone ZIP/postal code (of registration) Country (of registration) State/province (of registration) City (of registration) Address (of registration) ZIP/postal code (of residence) Country (of residence) State/province (of residence) City (of residence) Address (of residence) Type of employment Qualification Total work experience, years	Created manually Imported from an Excel file	GDPR Article 4 (1) **Products**: lending

		Total work experience, months Employer Legal form Industry Business phone Role Job title Length of employment, years Length of employment, months ZIP/postal code (of employment) Country (of employment) State/province (of employment) City (of employment) Address (of employment) Income Expenses Loans and guarantees Owned property		

Bpm'online functions involved in personal data processing

No.	Bpm'online function	Notes
1	Global search	Personal data display in the search results
2	Contact data enrichment	Adding new contact information to the contact page from an email chain Enriching contact data from their public profiles in social networks
3	Bulk emails	Adding a contact to the target audiences of a bulk email
4	Events	Adding a contact to the target audiences of a marketing event
5	Exporting analytical reports	Provided the list of displayed information includes personal data (such as top 5 opportunities where the customer names are mentioned, "List" and "Chart" dashboard components, etc.)
6	Identification of contacts from incoming calls	Contact identification by phone number Connecting a call with an existing contact record
7	Identification of contacts during lead qualification	Connecting a lead to an existing contact record
8	Duplicate record search and merging	Searching for duplicate contact records and merging them
9	(Pharma) Planning of visits	Adding a contact to the contact list during planning of visits
10	Generating a list of account's contacts	Contact identification when generating a list of account's contact persons
11	Viewing list in the [Contacts] section	Personal data is displayed in the list and in pop-up summaries
12	Opening a contact page from any location in bpm'online	Personal data is displayed on the page