absorb

GDPR Compliance

Procedures & Framework

November 2020

Intentionally left blank

Summary

The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC and was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens data privacy and to reshape the way organizations across the region approach data privacy.

Enforcement date: **25 May 2018** - at which time those organizations in non-compliance may face heavy fines.

The aim of the GDPR is to protect all EU citizens from privacy and data breaches in an increasingly data-driven world that is vastly different from the time in which the 1995 directive was established. Although the key principles of data privacy still hold true to the previous directive, many changes have been proposed to the regulatory policies; the key points of the GDPR as well as information on the impacts it will have on business can be found below.

Increased Territorial Scope (extra-territorial applicability)

Arguably the biggest change to the regulatory landscape of data privacy comes with the extended jurisdiction of the GDPR, as it applies to all companies processing the personal data of data subjects residing in the Union, regardless of the company's location. Previously, territorial applicability of the directive was ambiguous and referred to data process 'in context of an establishment'. This topic has arisen in a number of high-profile court cases. GDPR makes its applicability very clear - it will apply to the processing of personal data by controllers and processors in the EU, regardless of whether the processing takes place in the EU or not. The GDPR will also apply to the processing of personal data of data subjects in the EU by a controller or processor not established in the EU, where the activities relate to: offering goods or services to EU citizens (irrespective of whether payment is required) and the monitoring of behaviour that takes place within the EU. Non-Eu businesses processing the data of EU citizens will also have to appoint a representative in the EU.

Penalties

Under GDPR organizations in breach of GDPR can be fined up to 4% of annual global turnover or **€20 Million** (whichever is greater). This is the maximum fine that can be imposed for the most serious infringements e.g. not having sufficient customer consent to process data or violating the core of Privacy by Design concepts. There is a tiered approach to fines e.g. a company can be fined **2%** for not having their records in order (article 28), not notifying the supervising authority and data subject about a breach or not conducting impact assessment. It is important to note that these rules apply to both controllers and processors -- meaning 'clouds' will not be exempt from GDPR enforcement.

Consent

The conditions for consent have been strengthened, and companies will no longer be able to use long illegible terms and conditions full of legalese, as the request for

consent must be given in an intelligible and easily accessible form, with the purpose for data processing attached to that consent. Consent must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form, using clear and plain language. It must be as easy to withdraw consent as it is to give it.

Data Subject Rights

Breach Notification

Under the GDPR, breach notification will become mandatory in all member states where a data breach is likely to "result in a risk for the rights and freedoms of individuals". This must be done within 72 hours of first having become aware of the breach. Data processors will also be required to notify their customers, the controllers, "without undue delay" after first becoming aware of a data breach.

Right to Access

Part of the expanded rights of data subjects outlined by the GDPR is the right for data subjects to obtain from the data controller confirmation as to whether or not personal data concerning them is being processed, where and for what purpose. Further, the controller shall provide a copy of the personal data, free of charge, in an electronic format. This change is a dramatic shift to data transparency and empowerment of data subjects.

Right to be Forgotten

Also known as Data Erasure, the right to be forgotten entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data. The conditions for erasure, as outlined in article 17, include the data no longer being relevant to original purposes for processing, or a data subjects withdrawing consent. It should also be noted that this right requires controllers to compare the subjects' rights to "the public interest in the availability of the data" when considering such requests.

Data Portability

GDPR introduces data portability - the right for a data subject to receive the personal data concerning them, which they have previously provided in a '*commonly use and machine readable format*' and have the right to transmit that data to another controller.

Privacy by Design

Privacy by design as a concept has existed for years now, but it is only just becoming part of a legal requirement with the GDPR. At its core, privacy by design calls for the inclusion of data protection from the onset of the designing of systems, rather than an addition. More specifically - *'The controller shall Implement appropriate technical and organizational measure in an effective way in order to meet the requirements of this Regulation and protect the rights of data subjects'*. Article 23 calls for controllers to hold and process only the data necessary for the completion of its duties (data

minimization), as well as limiting the access to personal data to those needing to act out the processing.

Data Protection Officers

Currently, controllers are required to notify their data processing activities with local Data Protection Addendum (DPAs), which, for multinationals, can be a bureaucratic nightmare with most Member States having different notification requirements. Under GDPR it will not be necessary to submit notifications / registrations to each local DPA of data processing activities, nor will it be a requirement to notify / obtain approval for transfers based on the Model Contract Clauses (MCCs). Instead, there will be internal record keeping requirements, as further explained below, and Data Protections Representative (DPR) appointment will be mandatory only for those controllers and processors whose core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale or of special categories of data or data relating to criminal convictions and offences. Importantly, the DPR:

- Must be appointed on the basis of professional qualities and, in particular, expert knowledge on data protection law and practices
- May be a staff member or an external service provider.
- Contact details must be provided to the relevant DPA.
- Must be provided with appropriate resources to carry out their tasks and maintain their expert knowledge.
- Must report directly to the highest level of management.
- Must not carry out any other tasks that could results in a conflict of interest.

The Process

The European Union Legislative Process:

There are three European authorities officially responsible for the legislative process, and two advisory bodies worth noting for their specific relation to data privacy:

Authoritative bodies:

European Commission

The European Commission is the EU's executive body. It represents the interests of the European Union as a whole through a total of 28 commissioners, one from each member state, and 23,000 staff members. The body works on the basis of collective decision-making in order to complete its roles of proposing legislation, enforcing European law (with the help of the Court of Justice), representing the EU internationally, setting objectives, and managing EU policies and the budget.

European Parliament

The European Parliament is the only body whose members are directly elected by the citizens of the EU. Its aim is to preserve democracy and represent the interests of the people. It holds powers over passing legislation, the EU budget, and the President and appointments of the Commission. It is made up of 751 members, elected to five-year terms, with representation based upon the population of each member state.

Council of Ministers of the European Union

The Council of the Ministers of the European Union represents the governments of each member state. Its shares the power of adoption for legislation and the budget with Parliament, and also coordinates policy for the individual member states as well as foreign and security policy for the Union. Based on proposals from the Commission, the Council is the authoritative body to conclude and sign off on international agreements. The council meetings are attended by representatives (either ministers or state secretaries) who have the right to commit their countries and cast their vote.

Advisory bodies

Article 29 Data Protection Working Party

The Article 29 Working Party is and advisory body set up under the Data Privacy Directive 95/46/EC and is composed of representatives of the national data protection authorities (DPA), the EDPS and the European Commission. Its role is to advise the Commission on general data protection matters as well as laws from the EU that may affect data privacy. It also promotes the uniform application of the Data Protection Directive across the entire EU.

European Data Protection Supervisor

The European Data Protection Supervisor is the independent supervisory authority set up in 2014 by the Parliament and Council to advise EU administrations on the processing of personal data as well as supervising these bodies to ensure compliance to their own regulations. The EDPS also handles complaints and monitors new technologies related to the processing of personal data.

GDPR at Absorb

Objectives

This Absorb GDPR Compliance booklet is aimed to provide our commitment to data protection and privacy as well as our approach to GDPR, ensuring that:

- Personal data is lawfully and appropriately collected, used, disclosed, retained, and disposed of; and
- Practices are in place and in compliance with GDPR

Actions

In order to meet GDPR compliance Absorb has taken initiative to build upon their policies and procedures to meet the following criteria:

1. Maintain governance structure
2. Maintain personal inventory and data transfer mechanisms
3. Maintain internal data privacy policy
4. Embed data privacy into operations
5. Maintain training and awareness program
6. Manage information security risk
7. Manage third-party risk
8. Maintain notices
9. Respond to requests and complaints from individuals
10. Monitor for new operational practices
11. Maintain data privacy breach management program
12. Monitor data handling practices

Absorb takes action to ensure the collection and processing of data is concise, transparent, intelligible, and easily accessible. Notices will be clear and in plain language (particularly if addressed to a child). Data collected will also be free of charge.

Additionally, privacy policies (Privacy Notice) are in place to address the following:

- What information is being collected?
- Who is collecting it?
- How is it collected?
- Why is it being collected?

- How will it be used?
- Who will it be shared with?
- What will be the effect of this on the individuals concerned?
- Is the intended use likely to cause individuals to object or complain?

Absorb must obtain consent from the user with respects to data collection and processing. Absorb ensures details of the privacy policy are easily displayed with e.g. Within the UI a message to the user may contain layers and hyperlinks for the user to inquire further information. Another technique used is “just-in-time” privacy notices, so when a user engages with a data field, relevant information is displayed at that time with a pop-up style hint.

Contents

1. Maintain Governance Structure

This section details the steps taken by Absorb to address the following:

1) Assign Responsibility for data privacy to an individual (e.g. Privacy Officer, Privacy Counsel, CPO, Representative).
2) Appoint a Data Protection Officer (DPO) or Data Protection Representative (DPR) in an independent oversight role.
3) Conduct an enterprise privacy risk assessment.

The details following abide to the GDPR Act Articles 24, 27, 37, 38 and 39.

Article	Description
24. Responsibility of the Controller	This Article requires the data controller to implement appropriate technical and organizational measures to ensure and be able to demonstrate compliance with the GDPR. The appropriateness of these measures is based on a risk the nature, scope, context, and assessment that takes into account the nature, scope, context, and purposes of the processing as well as the risks of varying likelihood and severity for the rights and freedoms of individuals. There is a specific reference that, where proportionate in relation to the processing activities, data protection policies shall be implemented.
27. Representatives of controllers or processors not established in the union	This Article states that in cases where a non–EU data controller or data processor is offering goods or services (paid or free) to EU data subjects, or is monitoring the behaviour of data subjects within the EU, the data controller or processor must designate in writing a representative in the EU. Exceptions apply.
37. & 38. Designation of the data protection officer	This Article provides that the data controller or the data processor shall designate a data protection officer ("DPR") in three circumstances. If they: 1. Are a public-sector body 2. Are a body which processes large amounts of special data (Articles 9 & 10) 3. Undertake large scale, regular & systematic.
39. Tasks of the data protections officer	This Article sets out the tasks of the DPR including having due regard to the risk associated with processing operations, taking into account the nature, scope, context, and purposes of processing

This privacy management activity addresses how organizations assign responsibility for the operational aspects of a privacy program to an individual.

Example evidence to demonstrate compliance:

1) Written mandate for the Representative to act on behalf of the controller or processor; or
2) Evidence of communication of the Representative, e.g. within a privacy notice or via a website.

Absorb Actions

Assign Responsibility for data privacy to an individual in the EU

Requirement

In certain circumstances, EU data protection law requires that the controller or the processor shall designate in writing a representative in the Union.

Impact & Risk

Some organizations that act as processors may consider this to be a burdensome requirement and an expense.

Processors of data must Understand if any local laws require us to do so either as a processor or controller

- Regular and systematic monitoring of data subjects on a large scale; or
- Processing Sensitive Personal Data on a large scale.

Comments

Over the long-term, the appointment of a DPR may help reduce the risk of non-compliance with the GDPR.

Actions:

Absorb has appointed a Data Protection Representative, including assignment of tasks. In order to achieve GDPR compliance, the assignment of the responsibility includes responding to data protection inquiries or requests from EU data subjects, clients or data protection authorities, addressing the resolution of conflicts of interest, and stressing the DPR's responsibility for oversight of all processing activities.

Absorb has appointed Dylan O'Brien as Data Protection Representative ("DPR") in Dublin, Ireland

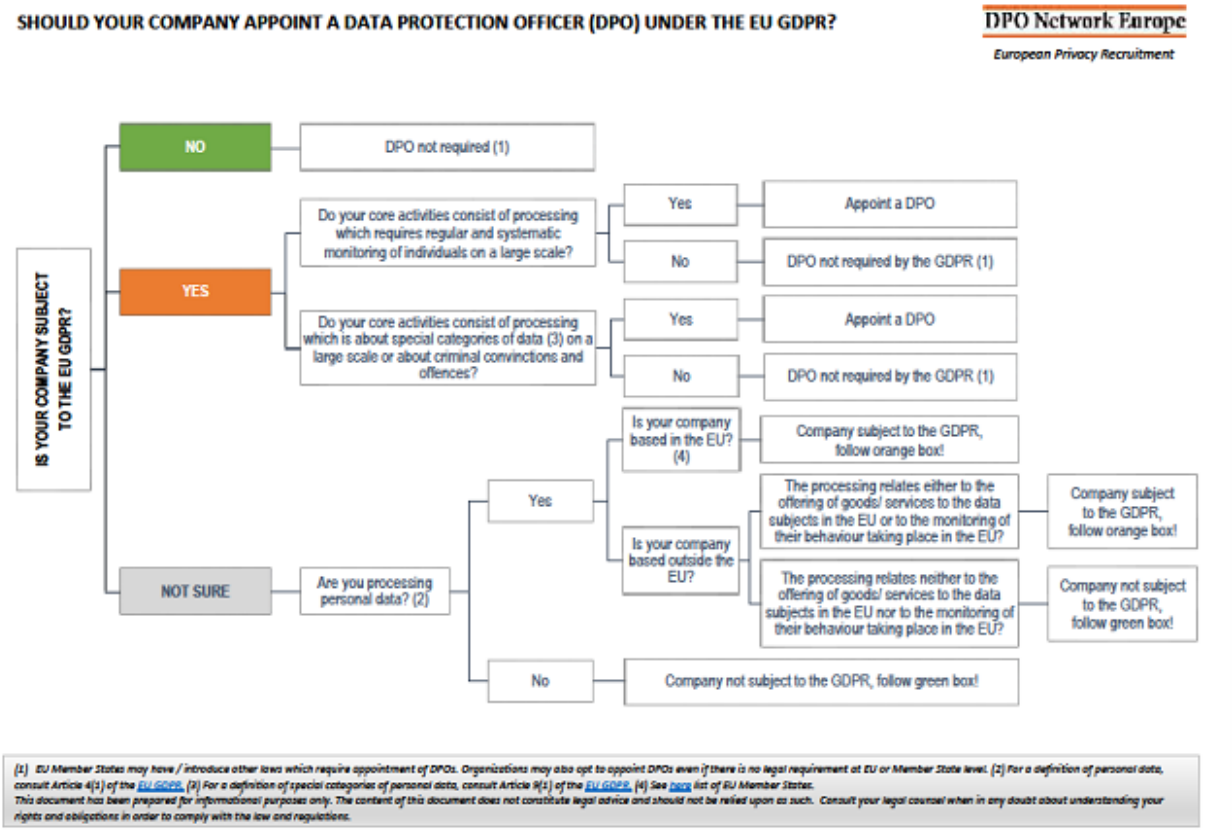
Dylan O'Brien
Data Protection Representative, EMEA
Address:
77 Sir John Rogerson's Quay
Block C Grand Canal Docklands, Dublin 2, D02 NP08
Dublin, Dublin 2
Ireland, Republic of
Tel: (+353) 87-653-3549
dylan.obrien@absorblms.eu

Absorb Actions:

Appoint a Data Protection Officer (DPO) in an independent oversight role

Requirement

When an organization is planning to engage in a form of processing that presents particular risks to the rights and freedoms of data subjects, that organization should consult the relevant DPA(s).



A DPO is a person who provides the primary contact point for data protection issues within an organization.

The WP29 has issued Guidelines on Data Protection Officers (WP 243)(the "DPO Guidelines") which provide further clarity on the key terms of Art 37, including "core activities", "large scale" and "regular and systematic monitoring".

Impact & Risk

The obligation to appoint a DPO may impose a significant burden, especially for smaller organizations.

The DPO Guidelines clarify that a single DPO can be appointed for a corporate group (or several entities within a group) provided that he or she is easily accessible from each business location for which he or she is responsible. Explicit permission to appoint a single DPO for a corporate group is a welcome development for organizations, but it will be important to ensure that such a DPO is provided with sufficient resources to perform the role.

Comments

Absorb's controller has appointed a DPR.DPO for cases where local laws require it to do so, or if its data processing activities involve:

- regular and systematic monitoring of data subjects on a large scale; or
- processing Sensitive Personal Data on a large scale.

A corporate group may collectively appoint a single DPO/DPR.

Organizations that are not required to appoint a DPR are free to do so voluntarily (although the DPO Guidelines note that a voluntary DPO is subject to the same requirements as mandatory DPO's). If a DPO/DPR is appointed, the organization must publish the details and communicate those details.

Controller & Processor of data between Absorb and Client must determine if core business operations involve regular and systematic monitoring of data subject on a large scale; and/or processing of sensitive personal data on a large scale.

Guidance

- The number of data subjects concerned - either as a specific number or as a proportion of the relevant population
- The volume of data and/or the range of different data items being processed
- The duration, or permanence, of the data processing activity
- The geographical extent of the processing activity

Examples of large-scale processing include:

- Processing of personal data for behavioral advertising by a search engine
- Processing of data (content, traffic, location) by telephone or internet service providers

Examples that do not constitute large-scale processing include:

- Processing of patient data by an individual physician
- Processing of personal data relating to criminal convictions and offences by an individual lawyer

Actions

Organizational wide, Absorb has appointed a Data Protection Officer (Privacy Officer) who acts independently and performs the tasks referred to in Article 39 by providing resources necessary to carry out those tasks.

Absorb Actions

Conduct an enterprise privacy risk assessment.

Conduct an Enterprise Privacy Risk Assessment. The scope of the privacy program is determined by the legal and regulatory compliance challenges and data impacted. In order to develop a privacy strategy, Absorb must:

1. Understand privacy compliance challenges in relevant laws, cultures, languages and business methods;

2. Identify areas where personal data is likely to be collected, processed or used, and any laws that apply to that type or handling of personal data; and

3. Determine based on these privacy-risks, what privacy priorities align with the organization's overall goals.

Actions

Absorb has a functional privacy office comprised of its Functional Departmental Team Leads, Governance Risk and Compliance team as well as the DPR.

The Privacy Office conducts an organizational privacy risk assessment across business units (including Human Resources, Sales, Marketing, Product Development, Client Services, etc.). The privacy risk assessment is a prerequisite for further development of an Organizational Privacy Program, in which the Privacy Office creates and oversees individual business unit privacy and security self-assessments, business process reviews, process improvements, communications and training.

The risk assessment process enables the Privacy Office to identify and prioritize privacy and security gaps across the organization and manage the privacy program for risk mitigation, compliance and to increase brand reputation and customer trust.

Out of scope are privacy risk assessments which are conducted by third parties in response to a privacy or data security breach or incident, or an audit conducted by internal compliance business units (e.g., internal audit of finance, ethics or other regulatory compliance).

2. Maintain Personal Data Inventory & Data Transfer Mechanisms

This section details the steps taken by Absorb to address the following:

1. Maintain an inventory of personal data holdings (what and where personal data is held).
2. Maintain records of the transfer mechanism used for cross boarder data flows (e.g. standard contractual clauses, approvals from regulators).
3. Use contracts as a data transfer mechanism.
4. Use adequacy or one of the derogations from adequacy (e.g. consent, performance of a contract, public interest) as a data transfer mechanism.
5. Use adequacy or one of the derogations from adequacy (e.g. consent, performance of a contract, public interest) as a data transfer mechanism.

The details following abide to the GDPR Act Article 30, 45, 46, 48, and 49.

Article	Description
30. Records of Processing Activities	This Article sets out a detailed list of information that must be maintained as records of processing activities carried out by and on behalf of the controller, as well as the requirement to make the records available to data subjects and Supervisory Authorities upon request. Exceptions apply.
45. Transfers on the basis of an adequacy decision	This Article provides that personal data may not be transferred to a third country or international organization without a specific authorization where the Commission has decided the country or organization ensures an adequate level of protection.
46. Transfer subject to appropriate safeguards	This Article states that in cases where a third country has not been assessed as providing an adequate level of data protection by the Commission, the data controller or processor may transfer personal data to a third country provided there are appropriate safeguards in place, enforceable data subject rights and legal remedies.
48. Transfers of disclosures not authorized by Union Law	This Article addresses when data controllers or processors may rely on a court judgment or tribunal decision in order to transfer personal data to a third country.
49. Derogations for specific situations	This Article enumerates derogations for specific situations that may support the transfer of personal data to a third country even in the absence of an adequacy decision or other appropriate safeguards. Among others, examples of derogations include explicit consent of the data subject or for the performance of a contract.

Absorb Actions

Maintain an inventory of personal data holdings

Absorb maintains a data mapping and inventory of personal data holdings (what personal data is held and where) organizational wide. Absorb creates and maintains an inventory of personal data holdings based on standard questionnaires for the various departments and IT Services where Absorb is deemed to be the data controller.

The inventory would address the different types of data held (the nature of employee data, customer data, client-owned data, and data co-owned with another organization) and where the personal data is held (e.g., servers, mobile devices, desktops, in the cloud, and geographic location). There are processes for updating the inventory to reflect changes related to the personal data maintained.

Absorb Actions

Maintain records of the transfer mechanism used for cross boarder data flows

Absorb maintains records of the transfer mechanism used for cross-border data flows (e.g. standard contractual clauses, approvals from regulators). Sending personal data abroad, even within the organization, can increase data protection risks and the complexity of managing them due to the differing privacy law requirements.

Absorb maintains documentation regarding all cross-border flows, tracking its use of, and compliance with, cross-border transfer mechanisms, such as:

- EU model clauses:
- EU adequacy decisions

Absorb Actions

Use contracts as a data transfer mechanism

Absorb uses contracts as a data transfer mechanism (e.g. Standard Contractual Clauses) Governments and regulators create model clauses to facilitate the transfer of personal data from a privacy-protective regime to a recipient in a country that does not provide adequate protections for personal data. When disclosing personal data to third parties in a country with inadequate privacy protections, Absorb uses these standard contractual clauses in its vendor contracts and processing agreements to ensure protection for personal data.

Absorb Actions

Use adequacy or one of the derogations from adequacy

Absorb uses adequacy or one of the derogations from adequacy (e.g. consent, performance of a contract, public interest) as a data transfer mechanism. When transferring personal data, Absorb ensure that recipients are located in jurisdictions that provide adequate protections for personal data. If the recipient is not in a jurisdiction that provides adequate protection, Absorb may still transfer personal data in accordance with a legal mechanism (e.g., Safe Harbor), or if the circumstances of the transfer fall within one of the exceptions from the requirement for adequate safeguards as set out in local law.

3. Maintain Internal Data Privacy Policy

This section details the steps taken by Absorb to address the following:

1) Document legal basis for processing personal data

The details following abide to the GDPR Act Articles 6, 9, 10.

Article	Description
6. Lawfulness of processing	This Article provides legal grounds on which personal data can be processed, as well as how to determine when further processing is compatible with the original purposes for processing.
9. Processing of special categories of personal data	This article sets out a general prohibition on the processing of sensitive data, followed by legal grounds on which sensitive personal data can be processed
10. Processing of personal data relating to criminal convictions and offences	This Article provides the legal basis upon which personal data relating to criminal convictions and offences may be processed.

Absorb Actions

Document legal basis for processing personal data as Controller

Absorb through its Privacy Notice is able to demonstrate a documented legal basis for processing personal data in some jurisdictions, Personal data may only be processed by Absorb in certain defined circumstances, e.g., with the data subject's consent, or where processing is necessary for the performance of a contract, etc. Given these limitations.

4. Embed Data Privacy into Operations

This section details the steps taken by Absorb to address the following:

1. Maintain policies and procedures for maintaining data quality
2. Maintain policies and procedure for secondary uses of personal data
3. Maintain policies and procedures for obtaining valid consent

The details following abide to the GDPR Act Articles 5, 6, 7, 8, 13, 14.

Article	Description
5. Principles relating to processing of personal data	This Article sets out the general principles that all processing activities must abide by, including: • Lawfulness, fairness and transparency • Purpose limitation • Data minimization • Accuracy • Storage or retention limitation • Integrity and confidentiality
6. Lawfulness of processing	This Article provides for the legal grounds upon which personal data can be processed, as well as how to determine when further processing is compatible with the original purposes for processing.
7. Lawfulness of processing	This Article sets out the standard for consent when relying on consent as a legal basis for processing personal data (demonstrable consent) and sensitive personal data (explicit consent).
8. Conditions applicable to child's consent in relation to information society services	This Article provides that where the legal basis of consent is being relied on in relation to offering information society services to minors under the age of 16 (or to younger children not younger than 13, if the age threshold is lowered by Member State law), verifiable parental consent must be obtained.
10. Information to be provided where personal data have not been collected from the data subject	This Article specifies what information is required to be provided o data subjects when that information is not obtained by the controller.
13. Information to be provided where personal data are collected from the data subject	This Article provides that where personal data relating to data subjects are collected, controllers must provide certain minimum information to those data subjects through an information notice. It also sets out requirements for timing of the notice and identifies when exemptions may apply.
14. Information to be provided where personal data have not been obtained	This Article specifies what information is required to be provided to data subjects when that information is not obtained by the controller.

from the data subjects	

Absorb Actions

Maintain policies and procedures for maintaining data quality

Absorb maintains data quality requirements, ensuring that information is accurate, complete and up-to-date.

Requirement
Data subjects are entitled to require a controller to rectify any errors in their personal data.

Absorb as a controller is obligated to correct or erase any inaccurate personal data. Absorb has a process to pull specific personal data and amend as requested or prompt the data subjects to review and amend periodically.

Impact & Risk
The position under the GDPR is largely unchanged, Absorb faces the same requirements under the GDPR as under the Directive, in relation to the right of rectification.

Comments
Controllers must ensure that inaccurate or incomplete data are erased or rectified. Data subjects have the right to rectification of inaccurate personal data.

Actions
Absorb, as a controller will correct or erase any inaccurate or incomplete data identified.

5. Maintain Training & Awareness Program

This section details the steps taken by Absorb to conduct privacy training. The details following abide to the GDPR Act Article 39.

Article	Description
39. Tasks of the data protections officer	This Article sets out the tasks of the DPO including having due regard to the risk associated with processing operations, taking

	into account the nature, scope, context, and purposes of processing

Absorb Actions

Maintain training and awareness programs

Absorb maintains a data privacy training program for its new and existing employees and continued re-enforcement of this program ensures that employees maintain an understanding of the organization's data privacy policies and practices.

Processes are in place to ensure that:

- Training content is updated and enhanced as required
- Training takes place on a regular basis, i.e., yearly
- The learning objectives are achieved
- Training attendance is documented

All employees are required annually and upon hire to complete Absorbs internal training modules.

6. Manage Information Security Risk

This section details the steps taken by Absorb to address the following:

1. Integrate data privacy into an information security policy
2. Maintain technical security measures (e.g. intrusion detection, firewalls, monitoring)
3. Maintain measures to encrypt personal data

The details following abide to the GDPR Act Articles 5, 32.

Article	Description
5. Principles Relating to Processing of Personal Data	This Article sets out the general principles that all processing activities must abide by, including: • Lawfulness, fairness and transparency • Purpose limitation • Data minimization • Accuracy • Storage or retention limitation • Integrity and confidentiality
32. Security of Processing	This Article states that organizations must implement an “appropriate” level of security based on the state of the art and costs of implementation, processing activities, and risk of varying likelihood and severity to individuals' rights and freedoms.

	The GDPR requires organizations to implement an “appropriate” level of security based on the state of the art and costs of implementation, processing activities, and risk of varying likelihood and severity to individuals' rights and freedoms. Examples are provided of measures that might be appropriate depending on the level of risk including regular tests of the effectiveness of security measures. The GDPR requires organizations to implement an “appropriate” level of security based on the state of the art and costs of implementation, processing activities, and risk of varying likelihood and severity to individuals' rights and freedoms. Examples are provided of measures that might be appropriate depending on the level of risk including encryption (32.1.a)

Absorb Actions

Integrate data privacy into an information security policy

Absorb has Integrated data protection into an information security policy. The Information Security Policy is a written statement that communicates the organization’s intent, objectives, requirements, responsibilities, and standards for protecting information.

The Policy:

- Is a high-level statement which clarifies the direction of, and support for information security
- Explains the “what”, “who” and “why” but not the “how” for protecting data
- Is supported by standards, guidelines, and operational procedures which explain in detail how to execute against the Policy requirements
- Is used to protect information assets from a wide range of threats to ensure business continuity, prevent security breaches, and reduce operational and business risk.

This privacy management activity focuses on the privacy-specific aspects of maintaining an Information Security Policy; the roles and responsibilities of the Information Security or IT organization are out of scope.

Absorb Actions

Maintain technical security measures

Absorb has Technical security measures and safeguards which are implemented to maintain, avoid, counteract or minimize security risks. Absorb has technical security measures consisting of hardware and software controls to provide automated protection to the system and applications.

Some examples of technical security measures include:

- Network segregation
- Firewalls
- Intrusion Detection System (“IDS”)
- Intrusion Prevention Systems (“IPS”)
- Anti-virus
- Access controls
- Security Event and Information Monitoring System

Absorb Actions

Maintain measures to encrypt personal data

Absorb has taken administrative security measures (i.e., procedural controls) and technical security measures (i.e., hardware and software controls) to guide the process of and transformation of personal data using an algorithm into an unreadable format, safeguarded against those who do not possess the encryption key.

The privacy management activity focuses on the privacy office's role in the encryption process and ensuring that personal data is encrypted in appropriate circumstances and in an appropriate fashion.

7. Manage Third Party Risk

This section details the steps taken by Absorb to address the following:

1. Maintain data privacy requirements for third parties (e.g. clients, vendors, processors, affiliates)
2. Maintain procedures to execute contracts or agreements with all processors
3. Conduct due diligence around the data privacy and security posture of potential vendors.

The details following abide to the GDPR Act Articles 28, 29, 32.

Article	Description
28. Processor	This Article creates an obligation on data controllers to only outsource processing to those entities that have sufficient guarantees to implement appropriate measures to guarantee GDPR compliance and to have a contract or binding act that governs the relationship. The contents of such a contract are set out.

	The Article also limits the ability of processors to subcontract without consent of the data controller, and what guarantees need to be in place in this arrangement.
29. Security of Processing	Processor This Article indicates that processors and staff of controllers and processors must only process personal data in accordance with either data controller instructions or a requirement of Union or Member State law.
32. Security of Processing	This Article states that organizations must implement an "appropriate" level of security based on the state of the art and costs of implementation, processing activities, and risk of varying likelihood and severity to individuals' rights and freedoms.

Absorb Actions

Maintain data privacy requirements for third parties

Data privacy laws continue to hold organizations accountable for protecting the privacy of any personal data accessed by third parties, including data processors, vendors, clients, and others who may receive personal data held. Absorb maintains internally--template clauses of the data protection requirements which third-parties must comply with.

Topics addressed in contracts include:

- Data protection responsibilities (e.g., acceptable use of personal data, use of subcontractors, restrictions on further disclosures or uses)
- Data security requirements
- Data disposal at contract-end
- Breach response obligations.

Absorb Actions

Maintain procedures to execute contracts or agreements with all processors

Absorbs privacy management activity relates to maintaining procedures to execute contracts or agreements with all vendors processing personal information in the custody of an organization, including:

- Identification of vendor contracts which require specific privacy provisions.
- Alternatives for structuring the legal relationships involved so privacy exists between all controllers and processors.

Absorb Actions

Conduct due diligence around the data privacy and security posture of potential Vendors and or Processors

When selecting potential vendors/processors, Absorb conducts an in-depth assessment of the third party's ability to perform the required activities in compliance with data protection laws and best practices. The third party's privacy and security posture are assessed to ensure it can adhere to the organization's data privacy policy and information security policy (this could be through an audit conducted by the organization or a third-party assurance report) and also ensure it meets our standards.

8. Maintain Notices

This section details the steps taken by Absorb to address the following:

1) Maintain a data privacy notice that details the organization's personal data and handling of said data.
2) Provide data privacy notice at all points where personal data is collected.

The details following abide to the GDPR Act Articles 8. 13. 14, 21.

Article	Description
8. Conditions applicable to child's consent in relation to information society services	This Article provides that where the legal basis of consent is being relied on in relation to offering information society services to minors under the age of 16 (or to younger children not younger than 13, if the age threshold is lowered by Member State law), verifiable parental consent must be obtained.
13. Information to be provided where personal data are collected from the data subject	This Article provides that where personal data relating to data subjects are collected, controllers must provide certain minimum information to those data subjects through an information notice. It also sets out requirements for timing of the notice and identifies when exemptions may apply.
14. Controllers obligations to provide notice where personal data have not been obtained from the data subject	This Article provides specifies what information is required to be provided to data subjects when that information is not obtained by the controller.
21. Right to Object	This Article addresses the right of data subjects to object to the processing of his or her personal data.

Absorb Actions

Maintain a data privacy notice that details the organization's personal data and handling of said data.

Absorb openly provides information related to its privacy policies and practices readily available to the public in a Data Privacy notice that identifies:

- What personal data is collected
- How the personal data is used, retained and disclosed
- What controls do the individuals whose personal data is involved have (e.g., what personal data is voluntary to provide, what opt-out options are available, and individual rights of access and correction).

Outside the scope of this privacy management activity are internal data privacy policies and mechanisms for providing the notice, i.e., this privacy management activity focuses on the content of the data privacy notice, not on the mechanisms of how to provide it.

Absorb Actions

Provide data privacy notice at all point where personal data is collected.

At each point where Absorb collects personal data (e.g. online, via text message, phone, in person, or employee application forms), the individual can review Absorbs data privacy notice or receive information about the privacy practices prior to providing personal data ("just in time" notice).

Outside the scope of this privacy management activity are the contents of privacy notices, i.e., this privacy management activity focuses on where to provide data privacy notices, not on the content of such notice.

9. Respond to Requests & Complaints from Individuals

This section details the steps taken by Absorb to address the following:

1. Maintain procedures to respond to requests for access to personal data.
2. Maintain procedures to respond to requests and/or provide a mechanism for individuals to update or correct their personal data.
3. Maintain procedures to respond to requests to opt-out of, restrict or object to processing.
4. Maintain procedures to respond to requests for data portability

5. Maintain procedures to respond to requests to be forgotten or for erasure of data

The details following abide to the GDPR Act Articles 7, 15, 16, 18, 19, 21.

Article	Description
7. Conditions for consent	This Article sets out the standard for consent when relying on consent as a legal basis for processing personal data (demonstrable consent) and sensitive personal data (explicit consent).
15. Right of access by the data subject	This Article addresses the right of data subjects to: obtain confirmation of whether their personal is being processed, where it is being processed and have access to the data. Additionally, it lists further information that should be supplied: • Purpose of processing • Categories of data • Recipients of data • Data storage period • ·Rights to rectification & complaint • Source of data • Existence of automated processing, associated logic and consequences · • Safeguards for transfer to third countries or international organizations. * Exception may apply (Article 23)
16. Right to rectification	This Article addresses the right of data subjects to obtain rectification of inaccurate data or completion of incomplete data.
19. Notification obligation regarding rectification or erasure of personal data or restriction of processing	This Article creates an obligation to notify each recipient to whom data has been disclosed of any rectification, erasure or restriction of processing. There is also an obligation to provide information to the data subject about these recipients upon request. *Exception may apply (Article 23)
21. Right to object	This Article addresses the right of data subjects to object to the processing of his or her personal data. * Exception may apply (Article 23)

Absorb Actions

Maintain procedures to respond to client or employee requests for access to personal data.

Absorb has processes for responding to requests by individuals for access to personal data stored and maintained about them that ensure the request is responded to completely and in a way that meets legal requirements around timing and content of a response.

The procedures include authenticating that the individual exercising the right of access has a legal right to do so (e.g., the data subject, a legal guardian, a parent of a minor child, or a legal heir or beneficiary of a decedent) as well as escalating complex access requests where first-responders are incapable of providing a response i.e. the client administrator is unable to fulfill the request by the data subject in the LMS.

Out of Scope are requests to correct or update personal data following a review of the personal data stored by the organization.

Absorb Actions

Maintain procedures to respond to client or employee requests and/or provide a mechanism for individuals to update or correct their personal data.

Where an individual believes his/her personal data should be corrected, rectified or updated due to accuracy or completeness concerns and has made a request for such correction or update, Absorb has procedures in place to:

- Investigate the need for updating or revision
- Make any appropriate changes
- Respond to the client administrator regarding the data subjects request and action taken

Absorb Actions

Maintain procedures to respond to client or employee requests to opt-out of, restrict or object to processing.

Absorb has procedures in place to:

- Accept requests made by client or employee to:
  - Opt-out of the use of their personal data;
  - Restrict the use of their personal data in certain processing such as making automated decisions, including profiling; or
  - Cease or block the use of their personal data.
- Process that request in a timely fashion
- Ensure the client or employee choice is executed within 30 days.

Allowing individuals to exercise an opt-out reflects the “choice” element of consent, by giving them a way of revoking permission to use their personal data. As part of the opt-out process, data subjects should receive information about the impact an opt-out may have, since some products or services may not be available as a result of the opt-out.

Mechanisms to opt-out of certain activities may be presented as part of Absorb’s privacy notice or be provided when the organization subsequently uses the personal data, e.g., at the bottom of a marketing communication and within our Privacy Notice.

Absorb Actions

Maintain procedures to respond to client or employee requests for data portability

The right of data portability goes beyond the data subjects traditional right to access personal data, and now provides a right to obtain data in a format that can be moved across electronic services or simply backed up by the data subject without hindrance, i.e., to obtain a readable version of their personal data.

In compliance with storing data electronically, Absorb has mechanisms in place for exporting and importing data from its systems, as well as process (automated and manual) for responding to requests by individuals for data portability.

Absorb can provide the data to the client through a secure process, and can be completed in one of the following ways:

- Encrypted data transfer through Hightail
- Encrypted emails
- Encrypted FTP’s

Absorb Actions

Maintain procedures to respond to client or employee requests to be forgotten or for erasure of data.

The right to be forgotten builds upon the notion in European data protection law that data subjects have a right to object to processing about them, and takes this notion one step further, to say that individuals not only can object to processing but also demand that data controllers erase or "forget" the data held about them.

Absorb has procedures in place to respond to requests to be forgotten, balancing the request against other fundamental freedoms, such as the right to access information and freedom of expression.

Absorb fulfills the request through a manual deletion process. The request is first received by HR, Marketing, Sales, etc. and then processed by Absorbs Integration team

who completes the hard deletion of the data subject. Upon deletion, Absorb confirms the request has been finalized with client or employee.

Please Note:

When deleting a Data Subject's (that is, an EU citizen who falls under the protection of the GDPR) Personal Identifiable Information (PII), it is required of a Data Controller (the Client) to ensure that all data is deleted everywhere. This includes in places like backups, shared drives, or with approved sub-processors.

Please contact your Absorb CSM to confirm that all data has been successfully deleted (erased) upon receiving a GDPR request from an eligible Data Subject."

10. Monitor for New Operational Practices

This section details the steps taken by Absorb to address the following:

1) Integrate privacy by design into system and product development.
2) Track and address data protection issues identified during Privacy Impact Assessment ("PIA") or Data Protection Impact assessment ("DPIA").
3) Report PIA/DPIA analysis and results to regulators (where/when required) and external stakeholders (if appropriate).

The details following abide to the GDPR Act Articles 25, 36.

Article	Description
25. Data protection by design and by default	This Article introduces responsibilities for the controller and requires data protection by design and by default. Data controllers must, at the time of determining the means of processing as well as when actually processing, implement appropriate technical and organizational measures (e.g., pseudonymisation) to implement the data protection principles set out in Article 5 (such as data minimization) and integrate necessary safeguards into the processing to meet the GDPR requirements. Data controllers must also implement data protection by default, i.e. implement appropriate technical and organizational measures to ensure that, by default, only personal data necessary for each specific purpose are processed. The concept of "necessary" informs the amount of data collected, extent of processing, and retention and accessibility of data. Data controllers must also implement data protection by default, i.e. implement appropriate technical and organizational measures to ensure that, by default, only personal data necessary for each

	specific purpose are processed. The concept of "necessary" informs the amount of data collected, extent of processing, and retention and accessibility of data.
36. Data protection impact assessment	This Article requires data controllers to assess the impact of processing operations on the protection of personal data where the processing is likely to result in a high risk for the rights and freedoms of data subjects.
36. Prior consultation	This Article requires data controllers to consult with the supervisory authority when a PIA indicates that processing would result in a high risk to data subjects and lists the minimum information the data controller needs to provide to the supervisory authority.

Absorb Actions

Integrate privacy by design into system and product development.

Increasingly, regulators have been calling for data protection by design and data protection by default to be embedded into data processing operations. This concept has even begun to appear in data protection legislation.

Absorb has a framework to help engineers, IT analysts, system architects, and application developers embed privacy-protective mechanisms into the fundamental design of systems and products.

Absorb has the following procedures, policies and actions in place to minimize the quantity of data to its specific needs.

- Privacy Impact Assessment
- Data Protection Impact Assessment
- Data Retention Policy
- Access Controls
- Encryption standards

Absorb Actions

Track and address data protection issues identified during PIA's/DPIA's

The privacy impact assessment ("PIA") or data protection impact assessment ("DPIA") needs to feed into planning a project's next steps. A procedure exists to:

- Evaluate the issues identified in the PIA/DPIA
- Assess possible protections and alternative processes to mitigate those data protection risks identified; and
- Track that the chosen mitigations are implemented.

The procedure ensures Absorb treats similar data protection issues consistently and allows for learning from one PIA/DPIA to be applied to subsequent PIAs/DPIAs.

Absorb Actions

Report PIA/DPIA analysis and results to regulators (where/when required) and external stakeholders (if appropriate).

Where a privacy impact assessment ("PIA") or data protection impact assessment ("DPIA") indicates that there are privacy risks that cannot be mitigated by reasonable means, or it might take additional time, it may be prudent (or required) under certain privacy and data protection laws to report the PIA to the relevant regulator or external stakeholders (e.g. customers, privacy advocates, etc.) so that these groups are made aware of the attendant data privacy risks prior to the launch of a new privacy product, program, system, process or the relocation of personal data to another jurisdiction. Depending on the industry and the applicable law, there may also arise situations where organizations are required to report their PIAs/DPIAs or make their PIAs/DPIAs publicly available.

Absorb has measure in place for contacting customers in these instances. Upon review Absorb will:

- Send PIA/DPIA findings to DPO.
- Absorb's DPO reviews findings for approval or not.
- If not approved, DPO presents findings to Data Protection Authority or external stakeholder for review or approval prior to executing the project.
- If "approved" DPO presents findings to Data Protection Authority for consent or consent with action to mitigate risk.

11. Maintain Data Privacy Breach Management Program

This section details the steps taken by Absorb to address the following:

1) Maintain a data privacy incident / breach response plan.
2) Maintain a breach notification (to affected individuals) and reporting (to regulators, credit agencies, law enforcement protocol).
3) Maintain a log to track data privacy incidents and or breaches.

The details following abide to the GDPR Act Articles 12, 33, 34.

Article	Description
12. Transparent information,	This Article requires that when data controllers are providing information to data subjects as part of breach notifications, the

communication and modalities for the exercise of the rights of the data subject	communication must be in a concise, transparent, intelligible, and easily accessible form, use clear and plain language. Information may be provided in writing, electronically (where appropriate), or orally (as long as identity of the data subject is verified).
33. Notification of a personal data breach to the supervisory authority	This Article makes it mandatory to notify supervisory authorities in the event of a data breach that poses a "risk of harm". The notification is expected without undue delay and where feasible within 72 hours. As well, detailed content requirements are set out for the notification letter. The circumstances of the data breaches must also be documented.
34. Communication of a personal data breach to the data subject	This Article requires notification to data subjects of breaches that result in a "high risk" for the rights and freedoms of individuals.
33. Notification of a personal data breach to the supervisory authority	Article 33.5 – States that the controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

Absorb Actions

Maintain a data privacy incident / breach response plan

Absorb has an incident/breach response plan that provides a coherent, systematic and proactive way of managing privacy breaches and security incidents that affect personal data in a consistent fashion.

Absorb Actions

Maintain a breach notification (to affected individuals) and reporting (to regulators, credit agencies, law enforcement) protocol.

Absorb creates and maintains a breach notification and reporting protocol that provides a plan for providing notifications of a data privacy incident to affected individuals, government agencies, regulators, and other external third parties in a timely manner. The plan ensures that notifications and reports align with legal requirements and best practices.

Absorb Actions

Maintain a log to track data privacy incidents and or breaches.

Absorb logs certain details regarding data privacy incidents or breaches for the purpose of determining information necessary for achieving compliance with breach notification laws, adhering to industry best practice, and being able to demonstrate such compliance in the event of a lawsuit or regulatory examination.

Outside the scope of this privacy management activity is the logging of data for IT security purposes, such as evaluating whether the incident is an isolated occurrence or reflective of system-wide failures or vulnerabilities

12. Monitor Data Handling Practices

This section details the steps taken by Absorb to address the following:

1) Maintain documentation as evidence to demonstrate compliance and or accountability.
2) Must maintain certifications accreditation, or data protection seals for demonstrating compliance to regulators.

    - While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this privacy management activity may produce additional documentation to help demonstrate compliance with GDPR Act Articles 5, 24.

The details following abide to the GDPR Act Articles 5, 24.

Article	Description
5. Principles Relating to Processing of Personal Data	This Article sets out the general principles that all processing activities must abide by, including: · Lawfulness, fairness and transparency · Purpose limitation · Data minimization · Accuracy · Storage or retention limitation · Integrity and confidentiality
24. Responsibility of the data controller	This Article requires the data controller to implement appropriate technical and organizational measures to ensure and be able to demonstrate compliance with the GDPR.

Absorb Actions

Maintain documentation as evidence to demonstrate compliance and or accountability.

By compiling and maintaining up-to-date documentation that reflects the state of the Absorb's privacy program; Absorb stands ready to demonstrate compliance with privacy and data protection laws, as well as being accountable for the functioning of the privacy program.

Absorb Actions

Must maintain certifications accreditation, or data protection seals for demonstrating compliance to regulators.

While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this privacy management activity may produce additional documentation to help demonstrate compliance with:

- Article 5 – Principles relating to processing of personal data
- Article 24 – Responsibility of the controller

Absorb has the following:

- DPA
- Data Breach Plan
- PIA / DPIA
- Documents and Records Control
- Privacy Policy
- Employee Data Protection Policy
- Privacy Notice
- Data Retention Policy
- DPR Job Description
- Records of Processing Activities
- Processor Data Map
- Consent Forms