

Arkadin Data protection & privacy white paper

Version May 2018



an NTT Communications Company

[Table of Contents]

| | |
|---|----|
| 1- About Arkadin | 4 |
| 2- Objectives | 6 |
| 3- What does the GDPR cover? | 8 |
| 4- What does the GDPR require? | 10 |
| 5- Who are the data processing players? | 15 |
| 6- What are GDPR players' obligations? | 16 |
| 7- Data subjects' rights | 18 |
| 8- Conclusion/Disclaimer | 20 |



[About Arkadin]

Arkadin is one of the largest and fastest growing global providers of cloud communications services in the world. Our collection of market-leading audio, web and video conferencing as well as Unified Communications solutions enables enjoyable collaboration experiences that are essential to success in a digitally connected global workplace.

As an NTT Communications company, one of the world's largest telecommunications companies, our services are delivered in the cloud and backed by a cutting-edge infrastructure for premium service quality.

Over **50,000** customers spanning the largest global enterprises to small businesses are supported locally in **19** languages through our network of 56 operations centers in **33** countries.

For more information visit:  www.arkadin.com



[Objectives]

Data protection is a long European story that started at the end of the 50's with the European convention of Human rights that adopted the fundamental right to privacy. With the creation of the first computer and the awakening of the internet, the European authorities decided to adopt one of the world's first major privacy laws in 1995: the EU's Data Protection Directive. This directive required companies to be transparent about their personal data processing, have a legitimate purpose for their use of that data and exercise care in handling data.

With rapid changes in technologies such as 'Cloud computing' being used around the world and the development of large companies processing huge amounts of personal data, an update was necessary. This is one of the reasons why EU legislators adopted the "General Data Protection Regulation" (GDPR) in 2016. This new European privacy law will keep privacy relevant in a world where far more data is collected than ever before.

On May 25, 2018, the GDPR has come into force and has replaced the 1995 EU Data Protection Directive. This new European privacy law (i) creates a new landscape for European data protection at a global level; (ii) intends to strengthen the rights that individuals have regarding personal data relating to them and (iii) seeks to unify data protection law across Europe, regardless of where data are processed.

The purpose of this document is to explain how Arkadin implements this new regulation.



What does the GDPR cover?

1- Personal Data – The GDPR expands and clarifies the concept of personal data but it largely remains the same.

‘**Personal Data**’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; (article 4 of the GDPR)

a Arkadin is likely to process personal data such as first name, last name, country, professional e-mail address, IP address, moderator pin code, participant pin code, web login, MAC address, billing address, and phone numbers. Arkadin does not process any special categories of personal data (Article 9 of the GDPR), neither personal data of children (article 8 of the GDPR).

2- Data Processing – The GDPR only applies to organisations that process personal data. It commonly refers to any automated or manual processing that involves personal data.

‘**Processing**’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction; (article 4 of the GDPR)

a Arkadin may process your personal data for a variety of legitimate purposes such as provisioning, reporting, billing, client/end-user support or for marketing activities. This data processing allows Arkadin to provide and support its services and make them continuously better for its clients.

3- Territorial Scope – The GDPR covers two situations.

- 1-** It covers any processing of personal data by an EU based company, regardless of whether the processing takes place in the EU or not.
- 2-** It covers any processing of personal data of individuals located in the EU by a company not based in the EU where the processing activities are related to the offering of services to such data subjects in the EU (application of the Extraterritoriality Principle).

‘**Territorial Scope**’ – This Regulation applies to:

- The processing of personal data in the context of the activities of an establishment of an organisation in **the Union**, regardless of whether the processing takes place in the Union or not; or
 - The processing of personal data of data subjects **who are in the Union** by an organization not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, or not; or (b) the monitoring of their behavior within the Union ; or
 - The processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law (article 3 of the GDPR).
- a** As a global organisation which process personal data from individuals located in the EU, all Arkadin subsidiaries are directly concerned by the GDPR.



What does the GDPR require?

Any organisation (within or outside the EU) which processes personal data of individuals located in the EU shall comply with the following GDPR principles.

1- Fair and Lawful processing with Transparency

"Personal data shall be processed lawfully, fairly in a transparent manner in relation to the data subject" (article 5 clause 1 (a) of the GDPR).

In a nutshell:

- **Fairness and transparency:** Arkadin shall process personal data fairly and provide data subjects with information about how and why their personal data is processed.
- **Lawful:** Arkadin shall only process personal data, lawfully where it has a valid legal basis. Data processing shall respect at least one of the following conditions (article 6 of the GDPR);
- Data subject consents to data processing. The GDPR defines consent as "any freely given, specific, informed and unambiguous indication of a data subject's wishes through a statement or clear affirmative action" (article 4 of the GDPR).
- As data controller, the client shall receive consent from the data subjects before processing data subjects' personal data and sending those personal data to Arkadin
- Data processing is necessary for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering into a contract;
- Data processing is part of a legal obligation to which the data controller is subject;
- Data processing protects vital interests of the data subject;
- Data processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller;
- Data processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data.

- a All the information related to data protection such as (i) personal data processed, (ii) data subjects, (iii) sub-processors involved in the processing, (iv) data importers, to whom Arkadin transfers personal data and all other related information, can be found in Arkadin's Data Processing Agreement (DPA) available on Arkadin's website.

2- Purpose Limitations

Arkadin shall only collect personal data for a specific, explicit and legitimate purpose (article 5 clause 1 (b) of the GDPR). Any subsequent processing should be compatible with that purpose unless Arkadin has obtained the individual's consent or the processing is otherwise permitted by law.

- a Arkadin may process your personal data for specified, explicit and legitimate purposes listed in the DPA available on Arkadin's web site, such as provisioning, reporting, billing, client/end-user support or for marketing activities.

Where Arkadin intends to further process the personal data for a purpose other than that for which the personal data were obtained, Arkadin will provide clients with information on that other purpose and with any further relevant information as referred to in article 14 of the GDPR prior to that further processing.

3- Data Minimisation

Any personal data collected shall be "adequate, relevant and limited to what is necessary in relation to the purpose for which personal data are processed" (article 5, clause 1 (c) of the GDPR). Regarding this principle, organisations shall be sure that they are only storing the minimum amount of personal data required for their purposes.

- a Arkadin undertakes not to collect more personal data than necessary to ensure the best support and services for their clients.

4- Data Accuracy

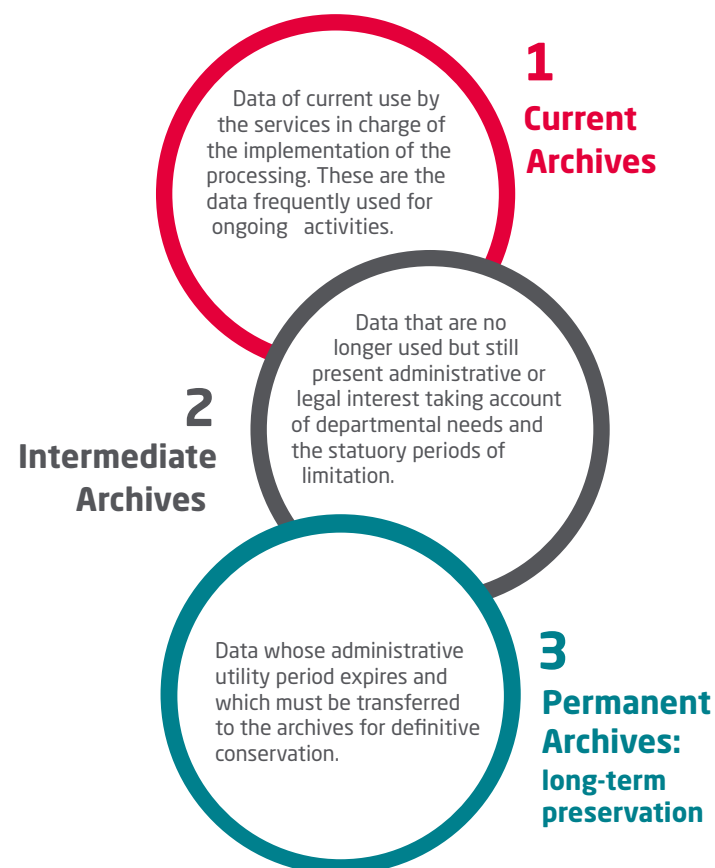
Data shall be "accurate, complete and where necessary kept up to date" (article 5, clause 1 (d) of the GDPR). Organisations are required to make sure information remains accurate, valid and fit for the purpose. This principle involves that organisations shall have processes and policies to address how they maintain the data they are processing and storing.

- a Arkadin and their employees are continually working on updating their personal data records (database) to ensure personal data accuracy.

5- Storage Limitations

Organisations shall only keep personal data for as long as it is needed for the purpose for which it was collected or for a further permitted purpose. (article 5, clause 1 (e) of the GDPR).

- a** In order to have an optimal overview on Arkadin's personal data processing and to meet legal and business data archival requirements, Arkadin sets up a data flow cartography and updates its data retention policy in accordance with the following pattern. Arkadin uses only current and intermediates archives to store personal data.



6- Integrity and Confidentiality

Personal data shall be handled "in a manner ensuring appropriate security including protection against unlawful processing or accidental loss, destruction or damage" (article 5, clause 1 (f) of the GDPR). Organisations that are collecting and processing personal data are responsible for implementing appropriate security measures that are proportionate to the security risks and rights of data subjects.

- a** The details about the appropriate security measures implemented by Arkadin are given in Schedule 2 of Arkadin's Data Processing Agreement.

7- Privacy by Design & Privacy by Default

Privacy by design (article 25 of the GDPR) - This principle means that when an organisation designs a new processing activity or develops a new service, this company shall follow GDPR principles such as minimisation, anonymisation and implementation of appropriate safeguards to protect privacy.

Privacy by default - Any organisation shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are

necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.

- a** All technical and organisational measures implemented by Arkadin are available in Schedule 2 of the DPA template.

8- Accountability

Any organisation that processes EU residents' personal data shall be responsible for and be able to demonstrate compliance with all the principles previously mentioned. This means:

- To set up technical and organisational measures to ensure and demonstrate compliance with the GDPR. These measures may include the appointment of a Data Protection Officer (DPO), the review of the security and data protection policies, staff training and regular audit of data processing.
- To maintain an adequate documentation on which data are processed, how, to what purpose, how long.

- To set up privacy by design and privacy by default mechanisms. This includes the application of principles of minimisation, pseudonymisation, transparency, etc.

- a** Arkadin's action plan to comply is set up around 4 main axes:

- Arkadin's policies and governance:**

Arkadin has updated its current code of conduct, privacy and cookies policies with regard to GDPR requirements. To be fully compliant, Arkadin appointed a DPO, a compliance board and chose the CNIL as supervisory authority. A dedicated email address has been created: privacy@arkadin.com

- Arkadin's data processing activities:**

Arkadin and its subsidiaries collect, store and process a variety of personal data related to individuals for business and legal reasons. Arkadin is committed to ensure that personal data are only processed when there is a legitimate basis for doing so and that any processing of personal data is fair and lawful. All of Arkadin's personal data processing is carefully stored in a record. Moreover, Arkadin now designs data protection into the development of every new project through a privacy by design strategy.

- Arkadin's contractual clauses:**

Arkadin offers a DPA template to its clients which meets the requirements of the GDPR. This DPA includes the processing details, the technical and organisational measures and the EU Standard Contractual Clauses (SCC) that enable personal data transfer outside the European Union in a compliant way.

- Arkadin's data protection awareness for employees:**

Arkadin believes that employees' awareness and skills regarding personal data are vital to its success. Therefore, Arkadin conducts a data protection training to its employees to raise their interest and train them about data protection and privacy.

The key principles for processing personal data:

- Fair and lawful with transparency
- Purpose limitation
- Minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability
- Privacy by design/default



Who are the data processing players?

The GDPR identifies different players in the data processing activities who will have either personal data rights or personal data obligations.

1- Data Subject

A data subject is a natural person to whom personal data relates. This data subject shall be located in the European Union to be protected by the GDPR. The main aim of the new European regulation is to strengthen the rights of these individuals who supply their personal data to organisations.

- a** In Arkadin, data subjects are commercial contact persons and users who attend audio, video, web, virtual event or unified communications conference calls. All the information regarding Arkadin's data subjects are available in Schedule 1 of Arkadin's DPA.

2- Data Controller

The data controller is a natural or legal person who determines the purposes for which and the manner in which any personal data are, or are to be, processed.

- a** As data controller, Arkadin clients determine the purposes and means of the personal data processing. More precisely, they determine the personal data Arkadin processes and stores on their behalf.

3- Data Processor

The data processor is any natural person or legal entity who processes data on behalf of the data controller.

- a** As data processor, Arkadin only processes personal data in accordance with the client's instruction and authorisation.

4- Data Sub-Processor

The sub-processor is any natural or legal person selected by the data processor that agrees to process personal data in accordance with the data processor's instructions.

- a** Even though Arkadin conducts the major part of data processing activities, Arkadin also engages third-parties to assist in supporting its services. Arkadin selects their sub-processors through a rigorous selection process to ensure they are able to provide Arkadin clients with the appropriate level of security and privacy. Arkadin makes information available about its sub-processors (including any third parties and any Arkadin affiliates) on its web page and undertakes to inform clients of any intended changes concerning any addition or replacement of sub-processors.

5- Data Importer

The data importer is a natural or legal person located outside EU which does not ensure adequate protection.

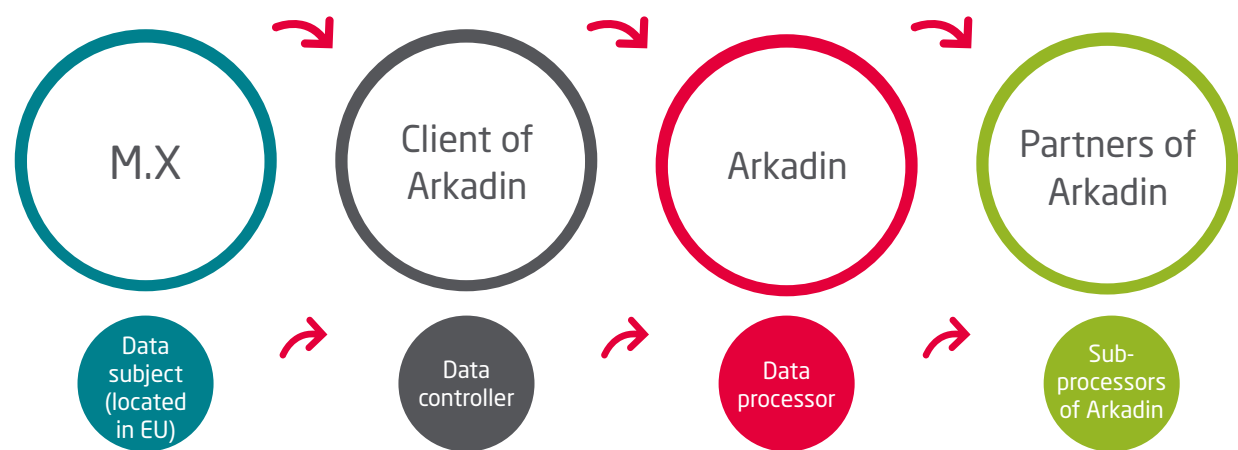
- a** Arkadin makes its data importers list available to its clients directly on its web page.

6- Data Exporter

The data exporter designates the data controller who transfers the personal data to processors or sub-processors established in third countries which do not ensure an adequate level of data protection.

What are GDPR players' obligations?

The GDPR has widely expanded the scope of data privacy regulation to any organisation that processes data of EU individuals, regardless their location. Therefore, Arkadin, their clients, and their suppliers shall comply to the GDPR and respect their respective obligations which differs depending on their role.



The GPDR fundamentally changes the balance of obligations and liabilities between the data controller and the data processor. Unlike the obligations under the Directive 95/46/CE, the GDPR sets up new obligations on the data processor that shall be met to be compliant in the processing of personal data.

1- Data Controller – The concept of a data controller is essentially unchanged under the GDPR and its obligations are quite similar.

In accordance with the GDPR, the data controller shall:

- Comply with the GDPR by adopting appropriate technical organisational measures which implement the data protection principles and respect the data protection by design and by default principles (articles 24 clause 1 and 25 of the GDPR);
- Demonstrate compliance with documentation that prove the measures adopted and their effectiveness (article 30 of the GDPR);

- Sign contracts with data processors that provide sufficient guarantees with regard to the technical and organisational measures (article 28 clause 1 of the GDPR);
- Record processing activities in order to demonstrate how and why personal data is being processed (article 30 clause 5 of the GDPR);
- Cooperate with the supervisory authority (article 57 of the GDPR);
- Notify the supervisory authority of personal data breach within 72 hours after becoming aware of (article 33 of the GDPR);

- Communicate any personal data breach to data subject without undue delay if this data breach is likely to result in a high risk to rights and freedoms of a natural person (article 34 of the GDPR);
- Carry out data protection impact assessment when the processing is likely to result in high risk to the rights and freedoms of the data subject (article 35 of the GDPR);

2- Data Processor – The GDPR imposes significant new obligations and responsibilities to the data processor. In accordance with the GDPR, any data processor shall:

- Process personal data only on data controller instructions; request (article 28 clause 3 (g) of the GDPR);
- Obtain written authorisation from the data controller before engaging a sub-processor (article 28 clause 2 of the GDPR), and take full liability for failures of any sub-processor to meet the GDPR requirements (article 28 clause 4 of the GDPR);
- Inform data controller about its sub-processors' identity (including any third party or any subsidiary) and inform about any intended changes concerning the addition or replacement of data sub-processors;
- Ensure personal data confidentiality;
- Maintain records of data processing activities;
- Delete or return all personal data to the data controller at the end of contract upon
- Contribute to compliance audits conducted by the data controller (article 28 clause 3 (h) of the GDPR);
- Use contract templates which are compliant with the GDPR rules and requirements;
- Ensure internal compliance audits on a regular basis;
- Notify the data controller without undue delay upon learning of data breaches (article 33 clause 2 of the GDPR).
- Provide appropriate safeguards in case of personal data transfer to third countries (article 46 of the GDPR);
- Promote internal privacy awareness campaigns through training sessions.

a Arkadin provides capabilities and contractual commitments created to meet these obligations through a Data Processing Agreement. This DPA is available to all Arkadin clients on the Arkadin compliance and ethics webpage: [link](#)

3- Data Sub-Processor – In the GDPR, the data processor shall not appoint data sub-processors without the prior written consent of the data controller.

The contract between Arkadin (as data processor) and Arkadin suppliers (as data sub-processor) contains the same data protection obligations as set out in the contract between the data processor (Arkadin) and the data controller (the client).

a In order to be GDPR compliant, Arkadin ensures to provide appropriate safeguards for the transfer of personal data to a third country, notably with the signature of standard contractual clause with its sub-processors.

[Data subject's rights]

In addition to considering applicable notice, consent and other requirements under the GDPR related to data collection and processing activities, the GDPR places a great deal of importance on data subjects' rights. The GDPR consolidates and strengthens existing rights for individuals by incorporating new rights and protections for data subjects, such as the right to erasure or to data portability, that bring a new perspective on the existing ones.

1- Right to Be Informed

(article 13, 14 and 34 of the GDPR)

This right compels organisations to provide “*fair processing information*”, like through a privacy notice. The GDPR requires organisations to provide more detailed information as to the “how and why” of the processing of personal data and on the rights of the data subjects. It also includes the right for the data subjects to be informed in the event of data breach to allow them to take appropriate action.

2- Right of Access

(article 15 of the GDPR)

Individuals have the right to obtain confirmation that their data are being processed and access them. The right of access gives a data subject the right to ask for a copy of their data in a human readable form.

3- Right to Rectification

(article 16 of the GDPR)

Individuals have the right to have inaccurate data corrected and/or incomplete data completed with supplementary data.

4- Right to Erasure

(article 17 of the GDPR)

Sometimes known as a “*right to be forgotten*”, individuals have the right to have personal data erased if the company has no lawful basis to continue processing the data. In some cases, or for some types of personal data, the company may decide not to erase the data but instead restrict its use (for example, it can only be used in the event of a legal claim).

5- Right to Restrict Processing

(article 18 of the GDPR)

Under the prior Directive, individuals had a right to “*block*” or suppress processing of their personal data. The restriction of processing under the GDPR is similar. When processing is restricted, it is permitted to store personal data but not further process it. It is allowed to retain just enough information about the individual to ensure that the restriction is respected in the future.

6- Right to Data Portability

(article 20 of the GDPR)

Individuals have the right to receive personal data which they provided to the organisation in a commonly used machine-readable format, so that they can share it with a different organisation.

7- Right to Object

(article 21 of the GDPR)

In some circumstances, individuals have the right to object to their personal data being used for a particular purpose. For example individuals can object to receive direct marketing or to be subject to a decision based only on automated processing.

8- Right to Not Be Subject to an Automated Individual Decision-Making

(article 22 of the GDPR)

The GDPR provides safeguards against the risk that a potentially damaging decision is taken without human intervention.

- a** Arkadin is committed to comply with the GDPR requirements and to respect data subjects' fundamental rights. Regarding those rights, Arkadin has a dedicated team to which data protection related enquiries may be directed. For any enquiries, please refer directly to: privacy@arkadin.com



[Conclusion]

Data privacy is a fundamental freedom for Arkadin clients and an undeniable trust factor for Arkadin. Therefore, Arkadin is strongly committed to comply with the GDPR, and sees this new regulation as a catalyst to deploy more secure and modern solutions via a privacy by design strategy. Respecting data protection principles is a top priority for Arkadin.

For any further questions about this white paper or about Arkadin's privacy commitments, feel free to contact the Arkadin compliance team at:

✉ privacy@arkadin.com

[Disclaimer]

This white paper constitutes an overview of the General Data Protection Regulation (GDPR) and how Arkadin interprets it. This document is provided only for informational purposes and does not provide legal advice. Clients and prospective clients shall consult their own legal counsel to understand the requirements of any law or regulation on their processing of personal data.

Arkadin reserves the right to make changes to this white paper at any time. Any change to this white paper will be prominently posted online and accessible via:

🌐 www.arkadin.com



[Enjoy work, enjoy life
Enjoy sharing]