



GDPR Master Procedure



Version	Date	Description	Author
1.0	2018	Creation of policy	Arkus
1.1	03-2019	Signature by the Board	Arkus
1.2	03-2020	Annual review	Arkus
1.3	01-2022	Annual review	L&C Department
1.4	03-2023	Annual review	L&C Department



I. Preamble

Arkus Financial Services (“Arkus”) having its registered office at 5, Rue Gabriel Lippmann, L-5365 Munsbach, Grand Duchy of Luxembourg is organized as a Limited Company. Arkus was incorporated on the 6 of September 2007 and is authorized by the Commission de Surveillance du Secteur Financier as “Professionnel du Secteur Financier” (“PSF”) articles 29-1 and 29-2 of the Law of 5 April 1993 on the financial sector, as amended.

Further to the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/ 46/ EC (General Data Protection Regulation) this document intends to implement the considerable changes applying immediately to Arkus. The GDPR draws a distinction between a data controller and a data processor in order to recognise that not all organisations involved in the processing of personal data have the same degree of responsibility. Each organisation should establish whether it is a data controller or a data processor for the same data processing activity or whether it is a joint controller.

II. Scope, purpose and users

This GDPR Master Procedure is based on globally accepted principles on data protection, ensuring trustworthy business relationships and Arkus’ reputation.

The Procedure lays out the general principles and actions for successfully managing the response to a data breach as well as fulfilling the obligations surrounding the notification to Supervisory Authorities and individuals as required by the EU GDPR.

All Directors, Employees/Staff, contractors or temporary Employees/Staff and third parties working for or acting on behalf of Arkus (“Company”) must be aware of, and follow this Procedure.

III. Legal and regulatory background

Arkus complies with the applicable legal and regulatory requirements and with the provisions of the *Commission de Surveillance du Secteur Financier* (“CSSF”) laid down in circulars and regulations, including but without limitations:

- ▶ EU GDPR 2016/679 (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC)
- ▶ Directive (EU) 2016/680 of 27 April 2016 (“Criminal Justice Directive”)
- ▶ Act of 11 August 1982 on the protection of provacy
- ▶ Amended Act of 2 August 2002, implementing Directive 95/46/EC has been **repealed**
- ▶ Act of 1 August 2018 on the organisation of the National Data Protection commission and the general data protection framework
- ▶ Act of 1 August 2018 on the protection of individuals with regard to the processing of personal data in criminal and national security matters
- ▶ Amended Act of 30 May 2005, implementing Directive 2002/58/EC (electronic communications)



IV. Definitions

Board	the board of directors of Arkus
CSSF	<i>Commission de Surveillance du Secteur Financier</i>
Data Controller	is the natural or legal person, public authority, agency or any other body, which alone or jointly with others, determines the purposes and means of the processing of personal data.
DPO	is the Data Protection Officer
Data Processor	is a natural or legal person, public authority, agency or any other body which processes personal data on behalf of a Data Controller.
Data Subject	shall mean the natural person whose Personal Data are being processed by the Data Processor
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC
Highly sensitive data	covers personal data concerning <ul style="list-style-type: none"> • racial or ethnic origin • trade union membership • religious or philosophical beliefs • political opinions health data • data on sex life • genetic data • biometric data • judicial data
Management	the management of Arkus
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 Regulation.
Personal Data Breach	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
Processing	means any operation or set of operations which is performed on personal data or on sets of personal data, whether 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.
Supervisory Authority	means an independent public authority which is established by a Member State pursuant to Article 51, which is for Luxembourg the <i>Commission Nationale pour la Protection des Donnees</i> (CNPD).

V. Policies and Procedures

This GDPR Master Procedure with the following schedules and appendices forms an integral part:

1. Schedule 1- Personal Data Protection Policy
2. Schedule 2 - Data Retention Policy
3. Schedule 3 - Data Breach Management Procedure

Appendix 1.1 -formulaire-cnpd-data-breach-notification-form

Appendix 1.2 - Data Breach Notification Form to the CNPD

Appendix 2 – Data Breach Register

4. Schedule 4 - Data Subject Request Procedure
- Appendix 1 - Data Subject Access Request Form

5. Schedule 5 - Continuous training procedure

6. Schedule 6 - Website

Appendix 1-Privacy Notice

Appendix 2-Cookie Notice

Appendix 3-Terms of use

VI. Validity and Review

This document is valid as of May 2018 as amended from time to time.

Arkus will review this procedure on an ongoing basis and revise it minimum on a yearly basis.

For updates in citation, and not material changes, the update can be performed immediately with the approval of the Executive Management of Arkus.

For further or material updates or modifications, the updated procedure will be presented to the Board of Directors for approval and become effective upon its approval.



VII. Approval by the Executive Management and the Board if applicable

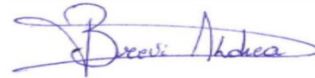
The Executive Management



Date: 13/04/2023
Name: Martin EWEN
Title: Chief Risk Officer



Date: 13/04/2023
Name: Andreas FUNK
Title: Conducting Officer



Date: 13/04/2023
Name: Andrea BREVI
Title: Conducting Officer