Data Protection Policy

CONTENTS

1. Document Control

1.1 Ownership

The Compliance Function~~, and Data Protection Officer are in association with the Data Protection Team, is~~ responsible for the~~development~~ and implementation of this document.

Document Owner: Data Protection Officer (DPO) is responsible for maintaining and updating the document and ensuring document is submitted for review in accordance with stated timetable.

1.2 Application

This Policy is intended to apply to Arena NV. Wherever local regulations are ~~more strict~~stricter than the~~requirements~~ set out in this Policy, the local standard ~~must~~will be applied.

Further details on jurisdictional or entity-specific requirements may be set out in appendices as needed.

This Policy applies to all staff employed ~~by, or~~by or working in an equivalent capacity under equivalent~~arrangements~~ such as contracts for services or temporary agreements, for the Company ("Staff").

1.3. Review and Approval

Adoption of this document by the Company is subject to the approval of the Board of Directors.

This document is subject to review and approval as set out in the table below.

Review 1	Review 2	Approval	Target Audience
Compliance Officer	Director or Senior Manager	Board of Directors	All staff

1. Document Control

1.1 Ownership

The Compliance Function~~,~~ and Data Protection Officer are ~~in association with the Data Protection Team, is~~ responsible for the~~development and implementation of this document.

Document Owner: Data Protection Officer (DPO) is responsible for maintaining and updating the document and ensuring document is submitted for review in accordance with stated timetable.

1.2 Application

This Policy is intended to apply to Arena NV. Wherever local regulations are ~~more strict~~stricter than the~~requirements set out in this Policy, the local standard ~~must~~will be applied.

Further details on jurisdictional or entity-specific requirements may be set out in appendices as needed.

This Policy applies to all staff employed ~~by, or~~by or working in an equivalent capacity under equivalent~~arrangements such as contracts for services or temporary agreements, for the Company ("Staff").

1.3. Review and Approval

Adoption of this document by the Company is subject to the approval of the Board of Directors.

This document is subject to review and approval as set out in the table below.

Review 1	Review 2	Approval	Target Audience
Compliance Officer	Director or Senior Manager	Board of Directors	All staff

1.4 Location

This document is located on the Company Intranet .

Target Audiences will be required to acknowledge receipt of this policy annually and when any significant changes are made.

1.5 *Maintenance*

This document shall be reviewed on an annual basis, and if any changes are proposed or recommended, the document will be updated and submitted for approval at that time. If there is a significant change to the governance structure, a material change in the market or macroeconomic conditions, or a request from the Board of Directors, review of this document may occur more frequently.

2. Scope and Purpose

2.1 Scope

This document outlines the Data Protection Policy of Arena NV (the 'Policy')

This Policy applies to the Company where a Data Subject's Personal Data is processed in the context of the business activities.

This Policy applies to all Processing of Personal Data in electronic form (including electronic mail and documents created with word processing software) or where it is held in manual files that are structured in a way that allows ready access to information about individuals.

This Policy has been designed to establish a baseline standard for the Processing and protection of Personal Data. Where national law imposes a requirement which is stricter than imposed by this Policy, the requirements in national law must be followed. Furthermore, where national law imposes a requirement that is not addressed in this Policy, the relevant national law must be adhered to.

If there are conflicting requirements in this Policy and national law, please consult with Compliance or the DPO for guidance.

If there are conflicting requirements in this Policy and national law, please consult with Compliance or the DPO for guidance.

2.2 Purpose

This purpose of this Policy is to:

- set out how the Company protects the personal information that we may hold about staff; clients; suppliers; and other third parties and what we do with that information;
- the rules on data protection and the legal conditions that must be satisfied when we collect, receive, handle, process, transfer and store personal data and ensuring staff understand our rules and the legal standards; and
- Clarify the responsibilities and duties of staff in respect of Data Protection and data security.

2.3 Definitions

- ***Binding Corporate Rules***
  Binding corporate rules means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity.

- ***Consent***
  Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
- ***Data Controller***

A data controller is an organisation that has full authority to decide how and why personal data is to be processed, and that has the overall responsibility for the data. This includes deciding on use, storage and deletion of the data.

- ***Data Subject***
  A Data Subject is an individual who is the subject of personal data.
- ***Personal Data***
  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.
- ***Privacy Impact Assessments***
  A Privacy Impact Assessment (PIA) is a process to help identify and minimise the data protection risks of a process / project. It is required for processing that is likely to result in a high risk to individuals. It should describe the nature, scope, context and purposes of the processing; assess necessity, proportionality and compliance measures; identify and assess risks to individuals and identify any additional measures to mitigate those risks.
- ***Processing***
  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.
- ***Profiling***
  Profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movement.
- ***Special Categories of Data***
  Special category data is personal data which the data protection law says is more sensitive, and so needs more protection. For example, information about an individual's race, ethnic origin, politics, religion, trade union membership, genetics, biometrics (where used for ID purposes), health, sex life; or sexual orientation.
- ***Third Party***
  Third Party means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

3. Governance

3.1 Data Protection Governance

The duties of the Data Protection Officer (DPOs) include:

- Informing and advising the Company and its employees who carry out Processing pursuant to Data Protection regulations, national law or other Data Protection provisions;
- Ensuring the alignment of this policy with Data Protection regulations, national law or other Data Protection provisions;
- Providing guidance with regards to carrying out Privacy Impact Assessments (PIAs);
- Acting as a point of contact for and cooperating with Data Protection Authorities (DPAs);

- Determining the need for notifications to one or more DPAs as a result of the Company's current or intended Personal Data Processing activities;
- Making and keeping current notifications to one or more DPAs as a result of the Company's current or intended Personal Data Processing activities;
- The establishment and operation of a system providing prompt and appropriate responses to Data Subject requests;
- Informing senior managers, officers, and directors of the Company of any potential corporate, civil and criminal penalties which may be levied against the Company and/or its employees for violation of applicable Data Protection laws.
- Ensuring establishment of procedures and standard contractual provisions for obtaining compliance with this policy by any Third Party who:
    - provides Personal Data to the Company
    - receives Personal Data from the Company
    - has access to Personal Data collected or processed by the Company.

3.2 Policy Dissemination & Enforcement

The management team of the Company must ensure that all employees responsible for the Processing of Personal Data are aware of and comply with the contents of this policy. In addition, the Company will make sure all Third Parties engaged to Process Personal Data on their behalf (i.e. their Data Processors) are aware of and comply with the contents of this policy. Assurance of such compliance must be obtained from all Third Parties, whether companies or individuals, prior to granting them access to Personal Data controlled by the Company.

3.3 Data Protection by Design & Default

To ensure that all Data Protection requirements are identified, reviewed and addressed:

- when designing new systems or processes for accessing or storing personal data;
- when reviewing or expanding existing systems or processes that store personal data;
- when developing strategies or policy that require privacy repercussions;
- when embarking on an data sharing initiative,

the Company must undertake an approval process before continuing and ensure that a PIA is conducted for all new and/or revised systems or processes for which it has responsibility.

Where applicable, the Information Technology (IT) department, as part of its IT system and application design review process, will work with the Data Protection Officer to assess the impact of any new technology uses on the security of Personal Data.

3.4 Compliance Monitoring

Formatted: Body Text, Space Before: 0,15 pt

To confirm that an adequate level of compliance is being achieved by the Company in relation to this Policy, Compliance will carry out an annual Business Handling Survey in conjunction with each relevant business function~~. and also compliance reviews of Third Parties[1].~~

The Data Protection Officer~~team~~, in cooperation with Compliance, Internal Audit and key business stakeholders, will devise a plan with a schedule for correcting any identified deficiencies within a defined and reasonable time frame. Any major deficiencies identified will be reported to and monitored by the Arena Executive Management team.

3.5 Data Privacy Principles

The Company has adopted the following principles to govern its collection, use, retention, transfer, disclosure and destruction of Personal Data:

3.5.1 Principle 1: Lawfulness, Fairness and Transparency

Personal Data shall be processed lawfully, fairly and in a transparent manner in relation to the Data Subject. This means the Company must tell the Data Subject what Processing will occur (transparency); the Processing must match the description given to the Data Subject (fairness); and it must be for one of the purposes specified in the applicable Data Protection regulation (lawfulness).

3.5.2 Principle 2: Purpose Limitation

Personal Data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. This means the Company must specify exactly what the Personal Data collected will be used for and limit the Processing of that Personal Data only tp what is necessary to meet the specified purpose.

3.5.3 Principle 3: Data Minimisation

Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are Processed. This means the Company must not store any Personal Data beyond what is strictly required.

3.5.4 Principle 4: Accuracy

Personal Data shall be accurate and, kept up-to-date. This means the Company must have processes in place for identifying and addressing out-of-date, incorrect and redundant Personal Data.

3.5.5 Principle 5: Storage Limitation

Personal Data shall be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data is Processed. This means the Company must, wherever possible, store Personal Data in a way that limits or prevents identification of the Data Subject.

3.5.6 Principle 6: Integrity & Confidentiality

Personal Data shall be processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful Processing, and against accidental loss, destruction or damage. The Company must use appropriate technical and organisational measures to ensure the integrity and confidentiality of Personal Data is maintained at all times.

~~[1] Third Parties review may take place on a longer cycle depending upon their risk rating. A third party that is classified as High will be subject to an annual survey; a Medium classified third party will be subject to a survey biennially; a Low classified third party will be subject to a survey triennially.~~

Formatted: Space Before: 0,5 pt

3.5.7 Principle 7: Accountability

The Data Controller shall be responsible for, and be able to demonstrate compliance. This means the Company must demonstrate that the six Data Protection Principles (outlined above) are met for all Personal Data for which it is responsible.

3.6 Data Collection

3.6.1 Data Sources

Personal Data should be collected only from the Data Subject unless one of the following apply:

- The nature of the business purpose necessitates collection of the Personal Data from other persons or bodies.
- The collection must be carried out under emergency circumstances in order to protect the vital interests of the Data Subject or to prevent serious loss or injury to another person.

If Personal Data is collected from someone other than the Data Subject, the Data Subject must be informed of the collection unless one of the following apply:

- The Data Subject has received the required information by other means.
- The information must remain confidential due to a professional secrecy obligation
- A national law expressly provides for the collection, Processing or transfer of the Personal Data.

Where it has been determined that notification to a Data Subject is required, notification should occur promptly, but in no case later than:

- One calendar month from the first collection or recording of the Personal Data
- At the time of first communication if used for communication with the Data Subject
- At the time of disclosure if disclosed to another recipient.

3.6.2 Data Subject Consent

The Company will obtain Personal Data only by lawful and fair means and, where appropriate, with the knowledge and Consent of the individual concerned. Where a need exists to request and receive the Consent of an individual prior to the collection, use or disclosure of their Personal Data, the Company is committed to seeking such Consent.

The Data Protection team, in cooperation with Compliance, Legal and other relevant business representatives, shall establish a system for obtaining and documenting Data Subject Consent for the collection, Processing, and/or transfer of their Personal Data. The system must include provisions for:

- Determining what disclosures should be made in order to obtain valid Consent.
- Ensuring the request for consent is presented in a manner which is clearly distinguishable from any other matters, is made in an intelligible and easily accessible form, and uses clear and plain language.
- Ensuring the Consent is freely given (i.e. is not based on a contract that is conditional to the Processing of Personal Data that is unnecessary for the performance of that contract).
- Documenting the date, method and content of the disclosures made, as well as the validity, scope, and volition of the Consents given.
- Providing a simple method for a Data Subject to withdraw their Consent at any time.

3.6.3 Data Subject Notification

appropriate to do so, provide Data Subjects with information as to the purpose of the Processing of their

Personal Data. When the Data Subject is asked to give Consent to the Processing of Personal Data and when any Personal Data is collected from the Data Subject, all appropriate disclosures will be made, in a manner that draws attention to them, unless one of the following apply:

- The Data Subject already has the information.
- A legal exemption applies to the requirements for disclosure and/or Consent.

The disclosures may be given orally, electronically or in writing. If given orally, the person making the disclosures should use a suitable script or form approved in advance by the DPO. The associated receipt or form should be retained, along with a record of the facts, date, content, and method of disclosure.

3.6.4 External Privacy Notices

Each website provided by the Company will include an online 'Privacy Notice' fulfilling the requirements of applicable law. All Privacy Notices must be approved by legal prior to publication on any website.

3.7 Data Use

3.7.1 Data Processing

Arena uses the Personal Data of its Contacts for the following broad purposes:

- The general running and business administration.
- To provide services to the customers.

The use of a contact's information should always be considered from their perspective and whether the use will be within their expectations or if they are likely to object.

Arena will process Personal Data in accordance with all applicable laws and applicable contractual obligations. More specifically, Processing of Personal Data will not be undertaken unless at least one of the following requirements are met:

- The Data Subject has given Consent to the Processing of their Personal Data for one or more specific purposes.
- 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.
- Processing is necessary for compliance with a legal obligation to which the Data Controller is subject.
- Processing is necessary in order to protect the vital interests of the Data Subject or of another natural person.
- 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.
- 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, in particular where the Data Subject is a child).

There are some circumstances in which Personal Data may be further processed for purposes that go beyond the original purpose for which the Personal Data was collected. When making a determination as to the compatibility of the new reason for Processing, guidance and approval must be obtained from

Compliance before any such Processing may commence.

Company will address the following additional conditions to determine the fairness and transparency of any Processing beyond the original purpose for which the Personal Data was collected:

- Any link between the purpose for which the Personal Data was collected and the reasons for intended further Processing.
- The context in which the Personal Data has been collected, in particular regarding the relationship between Data Subject and the Data Controller.
- The nature of the Personal Data, in particular whether Special Categories of Data are being Processed, or whether Personal Data related to criminal convictions and offences are being Processed.
- The possible consequences of the intended further Processing for the Data Subject.
- The existence of appropriate safeguards pertaining to further Processing, which may include Encryption, Anonymisation or Pseudonymisation.

3.7.2 Special Categories of Data

In any situation where Special Categories of Data are to be Processed, prior approval must be obtained from the Office of Data Protection and the basis for the Processing clearly recorded with the Personal Data in question. Where Special Categories of Data are being Processed, the Company will adopt additional protection measures. The Company may also adopt additional measures to address local custom or social expectation over the Processing of Special Categories of Data.

3.7.3 Children

Children are unable to Consent to the Processing of Personal Data. Consent must be sought from the person who holds parental responsibility over the child. However, it should be noted that where Processing is lawful under other grounds, Consent need not be obtained from the child or the holder of parental responsibility.

Should the Company foresee a business need for obtaining parental Consent for services offered directly to a child, guidance and approval must be obtained from Compliance or the DPO before any Processing of a child's Personal Data may commence.

3.7.4 Data Quality

The Company will adopt all necessary measures to ensure that the Personal Data it collects and Processes is complete and accurate in the first instance, and is updated to reflect the current situation of the Data Subject.

The measures adopted by the Company to ensure data quality include:

- Correcting (Correction may include data erase and replacement with corrected or supplemented data.)
- Personal Data known to be incorrect, inaccurate, incomplete, ambiguous, misleading or outdated, even if the Data Subject does not request rectification.
- Keeping Personal Data only for the period necessary to satisfy the permitted uses or applicable statutory retention period.
- The removal of Personal Data if in violation of any of the Data Protection principles or if the Personal Data is no longer required.
- Restriction, rather than deletion of Personal Data, insofar as:
    - a law prohibits erasure.
    - erasure would impair legitimate interests of the Data Subject.

ascertained whether their information is correct or incorrect.

3.7.5 Profiling & Automated Decision-Making

The Company will only engage in Profiling and automated decision-making where it is necessary to enter into, or to perform, a contract with the Data Subject or where it is authorised by law. Where the Company utilises Profiling and automated decision-making, this will be disclosed to the relevant Data Subjects. In such cases the Data Subject will be given the opportunity to:

- Express their point of view.
- Obtain an explanation for the automated decision.
- Review the logic used by the automated system.
- Supplement the automated system with additional data.
- Have a human carry out a review of the automated decision.
- Contest the automated decision.
- Object to the automated decision-making being carried out.

The Company must also ensure that all Profiling and automated decision-making relating to a Data Subject is based on accurate data.

3.7.6 Digital Marketing

As a general rule, the Company will not send promotional or direct marketing material through digital channels such as mobile phones, e-mail and the Internet, without first obtaining the recipient's Consent.

Where Personal Data Processing is approved for digital marketing purposes, the Data Subject must be informed at the point of first contact that they have the right to object, at any stage, to having their data Processed for such purposes. If the Data Subject puts forward an objection, digital marketing-related Processing of their Personal Data must cease immediately and their details should be kept on a suppression list with a record of their opt-out decision, rather than being completely deleted.

It should be noted that where digital marketing is carried out in a 'business to business' context, there is no legal requirement to obtain an indication of Consent to carry out digital marketing to individuals provided that they are given the opportunity to opt-out.

3.8 Data Retention

To ensure fair Processing, Personal Data will not be retained by the Company for longer than necessary in relation to the purposes for which it was originally collected, or for which it was further Processed.

The length of time for which the Company needs to retain Personal Data is set out in the approved retention list. This takes into account the legal and contractual requirements that influence the retention periods. All Personal Data should be deleted or destroyed as soon as possible where it has been confirmed that there is no longer a need to retain it.

3.9 Data Protection

The Company will adopt physical, technical, and organisational measures to ensure the security of Personal Data. This includes the prevention of loss or damage, unauthorised alteration, access or Processing, and other risks to which it may be exposed by virtue of human action or the physical or natural environment.

The minimum set of security measures to be adopted by Arena is provided in the Group 'Information Security Policy'.

3.10 Data Subject Requests

Arena will facilitate the exercise of Data Subject rights related to:

- Information access.
- Objection to Processing.
- Objection to automated decision-making and profiling.
- Restriction of Processing.
- Data portability.
- Data rectification.
- Data erasure.

If an individual makes a request relating to any of the rights listed above, the Company will consider each such request in accordance with all applicable Data Protection laws and regulations. No administration fee will be charged for considering and/or complying with such a request unless the request is deemed to be unnecessary or excessive in nature.

Data Subjects are entitled to obtain, based upon a request made in writing and upon successful verification of their identity, the following information about their own Personal Data:

- The purposes of the collection, Processing, use and storage of their Personal Data;
- The source(s) of the Personal Data, if it was not obtained from the Data Subject;
- The categories of Personal Data stored for the Data Subject.
- The recipients or categories of recipients to whom the Personal Data has been or may be transmitted, along with the location of those recipients.
- The envisaged period of storage for the Personal Data or the rationale for determining the storage period.
- The use of any automated decision-making, including Profiling.
- The right of the Data subject to:
    - object to Processing of their Personal Data.
    - lodge a complaint with the Data Protection Authority.
    - request rectification or erasure of their Personal Data.
    - request restriction of Processing of their Personal Data.

All requests received for access to or rectification of Personal Data must be directed to a DPO, who will log each request as it is received. A response to each request will be provided within one calendar month of the receipt of the written request from the Data Subject. Appropriate verification must confirm that the requestor is the Data Subject or their authorised legal representative. Data Subjects shall have the right to require the Company to correct or supplement erroneous, misleading, outdated, or incomplete Personal Data.

3.11 Law Enforcement Requests & Disclosures

In certain circumstances, it is permitted that Personal Data be shared without the knowledge or Consent of a Data Subject. This is the case where the disclosure of the Personal Data is necessary for any of the following purposes:

- The prevention or detection of crime.
- The apprehension or prosecution of offenders.
- The assessment or collection of a tax or duty.
- By the order of a court or by any rule of law.

If the Company Processes Personal Data for one of these purposes, then it may apply an exception to

the Processing rules outlined in this Policy, but only to the extent that not doing so would be likely to prejudice the case in question.

If the Company receives a request from a court or any regulatory or law enforcement authority for information relating to a Contact, you must immediately notify a DPO who will provide comprehensive guidance and assistance.

3.12 Data Protection Training

All Employees that have access to Personal Data will have their responsibilities under this Policy outlined to them as part of their staff induction training. In addition, the Company will provide Data Protection training and procedural guidance for their staff.

3.13 Data Transfers

The Company may transfer Personal Data to internal or Third Party recipients located in another country where that country is recognised as having an adequate level of legal protection for the rights and freedoms of the relevant Data Subjects.

Where transfers need to be made to countries lacking an adequate level of legal protection (i.e. Third Countries), they must be made in compliance with an approved transfer mechanism. The Company may only transfer Personal Data where one of the transfer scenarios list below applies:

- The Data Subject has given Consent to the proposed transfer.
- The transfer is necessary for the performance of a contract with the Data Subject.
- The transfer is necessary for the implementation of pre-contractual measures taken in response to the Data Subject's request.
- The transfer is necessary for the conclusion or performance of a contract concluded with a Third Party in the interest of the Data Subject.
- The transfer is legally required on important public interest grounds.
- The transfer is necessary for the establishment, exercise or defence of legal claims.
- The transfer is necessary in order to protect the vital interests of the Data Subject.
- The transfer is necessary for the conclusion or performance of a contract concluded with a Third Party in the interest of the Data Subject.
- The transfer is legally required on important public interest grounds.
- The transfer is necessary for the establishment, exercise or defence of legal claims.
- The transfer is necessary in order to protect the vital interests of the Data Subject.

3.13.1 Transfers between Group Entities

There may be occasions when it is necessary to transfer Personal Data from the Company to another Group Company or ~~Subsidiary~~Group Company, or to allow access to the Personal Data from an overseas location. Should this occur, the Company sending the Personal Data remains responsible for ensuring protection for that Personal Data.

Arena handles the transfer of Personal Data between Group Companies~~Subsidiaries~~, where the location of the recipient Entity is a Third Country, using the Binding Corporate Rules transfer mechanism. Binding Corporate Rules provide legally binding, enforceable rights on Data Subjects with regard to the Processing of their Personal Data and must be enforced by each approved Group Company~~Subsidiary~~, including their employees.
When transferring Personal Data to another Group Company located in a Third Country, you must:

- ~~Ensure that the recipient Subsidiary is included on the approved list of Enstar Group Entities subject to the Group 'Binding Corporate Rules Agreement'. The approved list is held and~~

~~maintained by Compliance.~~
transfer (for example, to fulfil a transaction or carry out a particular service).

- Ensure adequate security measures are used to protect the Personal Data during the transfer (including password-protection and Encryption, where necessary).

3.13.2 Transfers to Third Parties

The Company will only transfer Personal Data to, or allow access by, Third Parties when it is assured that the information will be Processed legitimately and protected appropriately by the recipient. Where Third Party Processing takes place, the Company will first identify if, under applicable law, the Third Party is considered a Data Controller or a Data Processor of the Personal Data being transferred.

Where the Third Party is deemed to be a Data Controller, the Company will enter into, in cooperation with the Data Protection Officer, an appropriate agreement with the Controller to clarify each party's responsibilities in respect to the Personal Data transferred.

Where the Third Party is deemed to be a Data Processor, the Company will enter into, in cooperation with the Data Protection officer, an adequate Processing agreement with the Data Processor. The agreement must require the Data Processor to protect the Personal Data from further disclosure and to only Process Personal Data in compliance with Group instructions. In addition, the agreement will require the Data Processor to implement appropriate technical and organisational measures to protect the Personal Data as well as procedures for providing notification of Personal Data Breaches.

When the Company is outsourcing services to a Third Party (including Cloud Computing services), it must identify whether the Third Party will Process Personal Data on its behalf and whether the outsourcing will entail any Third Country transfers of Personal Data. In either case, it must include adequate provisions in the outsourcing agreement for such Processing and Third Country transfers. ~~The Company has a 'Third Party Contact Checklist and Clauses' document[2] that should be used for guidance.~~

The Data Protection Officer will review Business Handling Surveys of Processing of Personal Data performed by Third Parties, especially in respect of technical and organisational measures they have in place. Any major deficiencies identified will be reported to and monitored by the Group Executive Management team.

3.14 Complaints Handling

The Data Protection team will inform the Data Subject of the progress and the outcome of the complaint within a reasonable period.

Data Subjects with a complaint about the Processing of their Personal Data should contact the ~~Complaints handler/~~Data Protection Officer via e-mail EEADataProtectionOfficer@castelmga.com. ~~(arena@arena-nv.be)~~

Arena will inform the Data Subject of the progress and the outcome of the complaint within a reasonable period.

~~2 Currently being finalised.~~
(DPA), Rue de la Presse 35, 1000 Brussels (https://www.dataprotectionauthority.be)

Formatted: Indent: Left: 1,16 cm

3.15 Breach Reporting

Any individual who suspects that a Personal Data Breach has occurred due to the theft or exposure of Personal Data must immediately notify the Office of Data Protection providing a description of what occurred. Notification of the incident can be made through the 'IT Service Desk' or via e-mail EEADataProtectionOfficer@castelmga.com.