AKKA PASSION FOR TECHNOLOGIES		Revision:	1
		Date:	05/2018
	Akka Group Personal Data Protection Policy	POLICY	

Introduction:

Akka Group is committed to comply with the requirements of the EU General Data Protection Regulation 2016/ 679 ("GDPR") in relation to how it holds and/or uses personal data.

Akka Group entities process many types of personal data for business and HR purposes concerning job applicants, employees, former employees, workers and contractors, partners, suppliers and customers. Akka Group is fully aware of its obligations under the GDPR to process personal data lawfully and to ensure that the rights of data subjects, as set out in GDPR, are observed correctly.

This policy sets out the rights of the aforementioned individuals as data subjects and the processes which should be followed in the event that the data subject wishes to exercise any such right.

Policy statement

All Akka Group employees are required to comply with their obligations under the GDPR, in relation to personal data about other employees, candidates, suppliers, partners and customers. Employees in positions that require use of personal data will be given separate specific guidance on these obligations and appropriate training. Employees must ask the Akka Data Protection Responsible in their organisation if they are unsure of their obligations.

If any employees fail to comply with these obligations, their failure will be regarded as serious misconduct under the Company's disciplinary procedure.

Policy Owner	Akka Group Privacy Team	
Issue Date	May 2018	
Revision number	1	

Table of Contents

1.Responsibilities

It is the responsibility of all line managers to ensure that they understand and communicate this Personal Data Protection policy to employees dealing with personal data. It is the responsibility of each employee to ensure that they understand this policy. The Data Protection responsible for each entity or country ultimately has accountability for the operation and monitoring of this policy. Human Resources shall provide support to the Data Protection responsible when required and will ensure that issues are dealt with consistently, promptly and fairly.

Management staff are responsible for ensuring that organizational, HR, and technical measures are in place so that any personal data processing is carried out in accordance with the GDPR.

Each Akka entity must identify their Data Protection responsible. The Data Protection responsible coordinates personal data protection for such entity, in cooperation with Akka Group Privacy Team. The responsibilities of the Data Protection Responsible include:

-Familiarize the employees with the content of the Akka Personal Data Protection policy.

-Promote the implementation and use of personal data processes and protection measures, in particular in case of processing of extremely sensitive personal data or transfers of personal data outside of the EEA.

-Ensure that their employees are sufficiently trained in personal data protection.

-Identify improper processing of personal data, or other violations of the data protection laws, and elaborate and escalate the necessary reports.

2.Employees Data Protection

2.1 Types of personal data held

The following types of personal data may be held by Akka entity, as appropriate, on its employees:

- conduct issues such as letters of concern, disciplinary proceedings
- CVs and other information gathered during recruitment
- holiday records
- internal performance information
- job title, job descriptions and pay grades
- medical or health information
- name, address, phone numbers - for the employee and next of kin
- National Insurance numbers
- references from former employers
- sickness absence records
- Bank details for payroll purposes
- Identification such as passport, drivers licence etc for right to work checks
- tax codes
- terms and conditions of employment
- training details.

Akka Group believes its use and storage of this personal data/information is consistent with the employment relationship and the principles of the GDPR. Akka entities need to store information about their employees for operational efficacy. Accordingly, this data will be held for management and administrative purposes, as

necessary, throughout employment, and for as long a period as is necessary following the termination of employment.

It may be necessary on occasion to disclose some personal data/information about employees to relevant third parties. The Akka entity may also transfer personal data/information to another Associated Company within the Akka Group, including to countries outside of the European Union, solely for purposes connected with the ongoing employment of the employee or efficient management of Akka's business activities.

2.2 Personal Data disclosures

The Akka Entity may be required to disclose certain personal data to a third person. The circumstances leading to such disclosures include:

- any employee benefits operated by third parties
- disabled employees - whether any reasonable adjustments are required to assist them at work
- employee's health data - to comply with health and safety or occupational health obligations towards the employee
- for statutory Sick Pay purposes
- HR management and administration - to consider how an employee's health affects his or her ability to do their job
- The smooth operation of any employee insurance policies or pension plans

These kinds of disclosures will only be made when strictly necessary for the purpose.

2.3 Acknowledgement of data processing

Employees will be informed of the Akka Personal data Protection policy at the moment they enter into labour relationship with Akka. A copy of Akka Group Personal Data Protection Policy will be added to the employment contract and all necessary resources will be in place to ensure employees understand their rights and obligations under this policy.

3. Customer and Partners Personal Data

3.1 Data processing for a contractual relationship or advertising

Personal data of the relevant prospects, customers and partners can be processed to establish, execute and terminate a contract. Also, if a Data Subject contacts Akka to request information about a service or product, data processing to meet this request is permitted.

If a Data Subject refuses the use of his/her data for advertising purposes, it can no longer be used for these purposes and must be blocked from use for these purposes.

3.2 Consent to Personal Data processing

In this case Personal Data for Customers and Partners can be processed following consent by the data subject. The declaration of consent must be obtained in writing or electronically for the purposes of documentation. In some circumstances, such as telephone conversations, consent can be given verbally. The granting of consent must be documented.

If personal data is collected, processed and used on websites or in apps, the data subjects must be informed of this in a privacy statement and, if applicable, in the information about cookies

If use profiles (tracking) are created to evaluate the use of websites and apps, the data subjects must always be informed accordingly in the privacy statement. Personal tracking may only be effected if it is permitted under national law or upon consent of the data subject. If tracking uses a pseudonym, the data subject should be given the chance to opt out in the privacy statement.

4. Data Subject rights

Under GDPR, all persons have the following rights in relation to their personal data:

- the right to be informed
- the right of access
- the right for any inaccuracies to be corrected
- the right to have information deleted
- the right to restrict the processing of the data
- the right to portability
- the right to object to the inclusion of any information
- the right to regulate any automated decision-making and profiling of personal data.

4.1 Right to be informed

Data Subjects have the right to be told how Akka processes their personal data and the reasons for the processing. Akka has develop this Akka Group Personal Data policy to explain what data will be collected, how Akka collects and processes it, what Akka processes it for and the lawful basis which permits Akka to process it. Data Subjects can obtain a copy of this policy from the website.

Akka Group also has specific privacy notices applicable to job applicants.

If Akka intends to use data already collected from a Data Subject for a different reason than that already communicated, Data Subject will be informed of the new reason in advance.

4.2 Right of access

Data Subjects have the right to access their personal data which is held by Akka. To request access to their personal data, Data Subjects can address their request to the following email address: *data-privacy@akka.eu*.

4.3 Right for data to be corrected or deleted

One of the fundamental principles underpinning data protection is that the data Akka processes about data Subjects will be accurate and up to date. Data Subjects have the right to have their personal data corrected if it is inaccurate or incomplete. If a Data Subject wishes to have his/her data rectified, he/she should do so by sending a request to the following email address: *data-privacy@akka.eu*

Data Subjects have the right to have their data deleted and removed from Akka systems where there is no compelling business reason for Akka to continue to process it.

Data Subjects have a right to have their personal data deleted in the following circumstances:

- where the personal data is no longer necessary in relation to the purpose for which Akka originally collected or processed it
- where Data Subject have withdrawn his/her consent to the continued processing of the data and there is no other lawful basis for Akka to continue processing the data
- where Data Subject objects to the processing and Akka has no overriding legitimate interest to continue the processing
- the personal data has been unlawfully processed
- the personal data has to be deleted due to a legal obligation.

If the Data Subject wishes to make a request for data deletion, he/she should send a request to the following email address: *data-privacy@akka.eu* .

Upon receipt of a request, Akka will delete the data unless it is processed for one of the following reasons:

- to exercise the rights of freedom of expression and information
- for Akka to comply with a legal requirement
- the performance of a task carried out in the public interest or exercise of official authority
- for public health purposes in the public interest
- archiving purposes in the public interest, scientific historical research or statistical purposes or
- the defence of legal claims.

Where the request of the Data Subject is not complied with because of the one of the above reasons, he/she will be informed of the reason. Where the request is to be complied with, the Data Subject will be informed when the data has been deleted.

Where the data which is to be deleted has been shared with third parties, Akka will inform those third parties where this is possible. However, where this notification will cause a disproportionate effect or imply disproportionate costs for Akka, this notification may not be carried out.

4.4 Making a Data Subject access request

Data Subject access requests to his/her personal data must be made in writing electronically by addressing an email to the following email address: *data-privacy@akka.eu*. Including specific details of the data that the Data Subject wishes to see will enable a more efficient response from Akka. Akka may need to contact the Data Subject for further details on his/her request if insufficient information is contained in the original request.

Akka will comply with the request without delay and at the latest within 30 working days from reception of the request unless one of the following applies:

- in some cases, Akka will be unable to supply certain pieces of information requested. This may be because it is subject to legal privilege or relates to management planning. Where this is the case, Akka will inform the Data Subject that his/her request cannot be complied with and an explanation of the reason will be provided
- Akka requires extra time because the requests are complex or numerous. In these circumstances, Akka will write by replying the email sent by the Data Subject within one month of receipt of the request to explain why an extension is required. Where an extension is required, information will be provided within three months of the request.

Data Subject requests will normally be complied with free of charge. However, Akka may charge a reasonable fee if the request is manifestly unfounded or excessive, or if it is repetitive. In addition, Akka may charge a reasonable fee if the Data Subject requests further copies of the same information. The fee charged will be based on the administrative cost of providing the information requested.

Akka may refuse to comply with a Data Subject access request if it is manifestly unfounded or excessive, or if it is repetitive. In these circumstances, Akka will write to the Data Subject without undue delay and at the latest within one month of receipt to explain why Akka is unable to comply. Data Subject will be informed of the right to complain about that.

5. Transfer of Personal Data

Transfer of personal data to recipients within the Akka Group is subject to the authorization requirements for processing personal data under the Data Transfer Agreement (DTA) signed by all entities of the Akka Group. The data recipient must be required to use the data only for the defined purposes and under the terms of such DTA.

In the event that data is transmitted to a recipient within the Akka Group to a country located outside of the European Union or outside the European Economic Area, such entity must agree to maintain the data protection level equivalent to this Data Protection Policy, as specified in the appropriate Annex 2 of the DTA signed by those entities.

If data is transmitted by a third party outside of the Akka Group, it must be ensured that the processing of such data fulfils the conditions of this Personal Data Policy, or similar conditions that respect the GDPR obligations.

6. Personal Data Processing security

Akka Group implements security measures to ensure the personal data processed is safeguarded from unauthorized access and unlawful processing or disclosure, as well as accidental loss, modification or destruction. This applies regardless of whether data is processed electronically or in paper form. Before the introduction of new methods of data processing, particularly new IT systems, technical and organizational measures to protect personal data must be defined and implemented. The technical and organizational measures for protecting personal data are part of Corporate Information Security Policy and must be adjusted continuously to the technical developments and organizational changes.

7. Monitoring of Personal Data protection obligations

Akka Personal Data Protection Policy is checked regularly at local and group level and under the responsibility of the Data Protection Responsible of each entity and the Akka Group. The results of the data protection controls must be reported to the Chief Compliance Officer.

8. Personal Data breaches and data protection incidents

All employees must inform immediately their supervisor, the Data Protection responsible in their entity or at Akka Group level, or the Chief Compliance Officer about breaches of this Personal Data Protection Policy and any protection incidents.

An internal report shall be completed to document any case of improper transfer of personal data to third parties, improper access by third parties to personal data, or the loss of personal data, in order to comply with the reporting duties.