DATA PROTECTION POLICY

For

ARCANOR A.Ş.

Version 1

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY

ARCANOR is a company that has cross-sectoral Data Fusion capabilities through aggregating multiple data sources in order to provide cutting edge solutions in advertisement sector to its customers.

ARCANOR fuses data provided from Mobile Applications with POIs, geospatial information etc. through machine learning and Data Fusion methods to create segmented audiences as well as insights by uploading custom audiences onto Marketing Platforms in order to make advertisement.

ARCANOR takes data privacy very seriously and is committed to protect Data Subjects' Personal Data. Within this scope, this Data Protection Policy outlines ARCANOR's collection, use, share, store and retention of Personal Data, its purposes and lawful basis of processing and Data Subject's data protection rights.

2. ADMINISTRATIVE INFORMATION

ARCANOR is a joint stock company established in Esentepe Talatpaşa Caddesi No:5 Harman Sok. 34394 Şişli/İstanbul, Turkey, registered in Istanbul Trade Registry with 295413-5 number.

ARCANOR's consultants and researchers are multi-lingual senior level management professionals with more than 10 years of experience within their relevant fields of operations.

More information can be found from the following website regarding ARCANOR:

https://www.arcanor.com

ARCANOR appointed a data protection officer whose details are as the following:

Name **:** Kaan Kalle

Email **:** legal@arcanor.com

3. SCOPE

3.1. Definitions:

Policy refers to this Data Protection Policy;

ARCANOR refers to the company stated in the Article 2 of this Policy;

Customer refers to natural persons and/or legal entities that render Services from ARCANOR;

Services means the services that ARCANOR provides to its customers including but not limited to insight services such as competition, market and Location analysis, marketing services in order to build audience segments for the marketing and advertising initiatives of audience partners and for supplying data to fuel the products;

Data Protection Regulations refers to GDPR -General Data Protection Regulation (*(EU) 2016/679*) and KVKK – Turkish Personal Data Protection Law numbered 6698;

Personal Data means any information identifying a Data Subject or information relating to a Data Subject that can identify (directly or indirectly) from that data alone or in combination with other identifiers or can reasonably be accessible. Personal Data excludes Anonymous Data or data that has the identity of an individual permanently removed;

Data Subject means the identified or identifiable Mobile App Users, Third Parties' Employees' Data, Personnels' Data or Web-site Visitors' Data to whom Personal Data relates;

Special Categories of Personal Data means information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data;

Criminal Convictions Data means personal data relating to criminal convictions and offences and includes personal data relating to criminal allegations and proceedings;

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;

Pseudonymised Data means placing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

Anonymous Data is the information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable that Data Protection Regulations do not concern its processing;

Re-identification is the process of matching anonymous data with publicly available information, or auxiliary data, in order to discover the individual to which the data belong.

Data Controller is the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with Data Protection Regulations;

Data Processor means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Data Controller;

Consent means an agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signify agreement to the Processing of Personal Data relating to them.

Automated Processing means any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing;

Profiling means to enable the analysis, determination and prediction of certain aspects of an individual’s personality or behaviour, interests and habits;

Personalized Advertisements means a marketing strategy by which companies leverage data analysis and digital technology to deliver individualized messages and product offerings to customers based on real-time and prolonged customer experiences;

Data Fusion means the aggregation and matching of multiple data sources through methods such as joining precisely or machine generated estimation of datasets sourced or stored from various data silos;

Data Partners means the third parties from whom ARCANOR provides data sets;

Data Providers means the Mobile Applications that collects data;

Mobile App User means the Data Subjects who uses Mobile Applications;

Third Parties' Employees means the contact persons of ARCANOR's **i)** Customers or **ii)** Data Partners and Data Providers, with whom ARCANOR communicates in order to fulfil its Services;

Personnels means the employees and shareholders of ARCANOR;

Web-site Visitors means persons who visit and leave their contact information to https://www.arcanor.com/contact;

Marketing IDs (MAID), such as GAID (Google Advertising ID) and IDFA (Identifier For Advertisers for IOS) or IFDV (for IOS 14) means resettable, random and unique identifiers formed as a string of characters for mobile devices which are collected for the purpose of Personalized Advertisements;

Mobile Software Development Kits (Mobile SDKs) means the software attached to Mobile Applications for the purpose of in-app analytics, data collection for Personalized Advertisements and other device related logs;

Location means geographic coordinates and objects retrieved through beacon, GPS, Wifi, cell tower triangulation or IP geolocation;

Mobile Application means downloaded and installed applications placed and offered on Apple Store or Google Playstore;

Point of Interests (POIs) means coordinates or set of coordinates that are machine or human generated, available open or closed-source which name and describe the features of a Location;

Digital Marketing means the process of marketing advertisements in bulk or in personalized segments throughout the mobile advertisement landscape;

Marketing Platforms are tools, such as search engines, social media, applications, email, and websites where Digital Marketing efforts take place.

Privacy Notice is a document that Data Controllers give to Data Subjects to explain how their Personal Data is processed in order to promote transparency and to give individuals more control over the way their data is collected and used;

Data Incident means any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that ARCANOR or its third-party service providers put in place to protect it.

4. DESCRIPTION OF PROCESSING

4.1. Data Flow Maps

See Annex-1 Data Flow Maps

4.2. Types of Data Subjects

Mobile App Users, Third Parties' Employees, Personnels, Web-site visitors

ARCANOR does not knowingly collect personal information from children under 16 years old or from websites or online services directed to children under 16 years old. Further, ARCANOR prohibits its Data Partners from providing ARCANOR with personal information from sites directed to children under the age of 16 or from consumers whose age these companies know to be under the age of 16.

4.3. Processing of Mobile App Users' Personal Data

4.3.1. Types of Personal Data

ARCANOR does not process Personal Data which can directly identify a person such as names, surnames, addresses, e-mail addresses or any kind of contact information.

It processes data which can identify a person in combination with other identifiers such as

- POI data, trademarks, agencies, shops, opponent locations
- Telco data (mobility, geographical location, internet usage)
- Online identifiers (IP, MAIDs)
- Mobile Apps' data (latitude, longitude, areas of interest)
- GPS data (latitude, longitude, time spent, time waited)
- Navigation data (vehicle, traffic speed, destination)
- Socio-economic data (income status, age, profession)
- Sectoral data (ADS-B, AIS, electricity consumption)
- Meta data (market prices, social media and Location)

ARCANOR does not process Special Categories of Personal Data or Criminal Convictions Data.

4.3.2. Sources of Personal Data:

The data is provided and aggregated through various direct integrations with Software Development Kits integrated by Data Partners and Data Providers that function in IOS and Android operating systems.

When Data Subject visits a Data Provider, they are asked for their Consent to use several data to personalize their advertising experience, which enables this data to be automatically sent to ARCANOR.

ARCANOR does not collect data from Mobile App Users directly.

Upon written request the list of Data Providers can be shared with Customers.

In cases where ARCANOR receives Personal Data of Data Subjects who reside in European Economic Area, ARCANOR is bound by the Standard Contractual Clauses for Controller to Controller transfers in the form approved by the European Commission (as amended or updated from time to time).

4.3.3. Purpose of Processing

ARCANOR fuses data provided from Mobile Applications with POIs, geospatial information etc. through machine learning and Data Fusion methods to create segmented audiences as well as insights by uploading custom audiences onto Marketing Platforms in order to make advertisement.

Within the advertisement purpose, ARCANOR performs Automated Processing including segmentation, clustering, evaluation, scoring, predicting audiences through large scale processing of data, creation of meta data and matching/combination of datasets.

4.3.4. Length and Frequency of Processing:

ARCANOR processes this type of data until its advertising function is over.

4.3.5. Data Minimisation:

ARCANOR purchases data from its Data Partners within the scope of its Services, in order to provide statistical insights, market analysis and clustered custom audiences to its Customers. ARCANOR uses aggregated, pseudonymised or anonymised data, machine learning algorithms and statistical analysis for the creation of custom audiences and insights. It does not obtain and/or store data that it does not use for marketing purposes in line with the requests of its Customers.

Only the competent Personnels being in relation to their role and duties are allowed to have access to such data where they need to in order to perform their job functions.

Data is not used in manner incompatible with marketing and/or statistical purposes.

4.4. Processing of Third Parties' Employees' Personal Data

4.4.1. Types of Personal Data

ARCANOR may process, name, surname, ID number, e-mail address, telephone number, authorized signatures lists, billing information of **i)** the Customer, -in cases where Customer is a natural person, **ii)** the employees of its Customers, Data Partners, Data Providers and/or its other suppliers.

ARCANOR does not process Special Categories of Personal Data or Criminal Convictions Data.

4.4.2. Sources of Personal Data:

Employees' Personal Data is obtained in physical and electronic form through the establishment of a commercial relationship.

4.4.3. Purpose of Processing

ARCANOR, processes Third Parties' Employees' Personal Data for communication purposes **i)** in rendering Services to its Customers, or **ii)** in obtaining services from Data Partners, Data Providers or its other suppliers. Privacy Notices shall be attached to the agreements executed between the parties.

4.4.4. Length and Frequency of Processing:

Personal Data of the employees are processed during the relationship between the parties in order to provide Service with and/or obtain service from third parties.

4.4.5. Data Minimisation:

ARCANOR obtains data from the Third Parties' within the scope of the commercial relationship with its Customers, Data Partners, Data Providers and/or other suppliers.

Only the competent Personnels being in relation to their role and duties are allowed to have access to such data where they need to in order to perform their job functions.

Data is not used in manner incompatible with the purpose stated in Art 4.4.3.

4.5. Processing of Personnels' Personal Data

4.5.1. Types of Personal Data

ARCANOR processes national id card, address, telephone number, passport, CV, diplomas, certificates, bank account details, blood type, medical certificate that is required by law.

4.5.2. Sources of Personal Data:

Personnels' Personal Data is obtained in physical and electronic form due to the establishment of an employment.

4.5.3. Purpose of Processing

ARCANOR processes Personnels' data in order to execute and fulfil the employment contract.

4.5.4. Length and Frequency of Processing:

Personnels' Personal Data is processed during their employment period and until the reason of processing is fulfilled provided that the legal responsibilities of ARCANOR are reserved.

4.5.5. Data Minimisation:

ARCANOR obtains data from its Personnels within the scope of its employment contracts.

Only the competent Personnels being in relation to their role and duties are allowed to have access to such data where they need to in order to perform their job functions.

Data is not used in manner incompatible with the purpose stated in Art 4.5.3.

4.6. Processing of Web-Site Visitors' Personal Data

ARCANOR may process name, surname and e-mail address, cookie ID of the Web-Site Visitors who would like to contact with ARCANOR. ARCANOR does not process Special Categories of Personal Data or Criminal Convictions Data.

4.6.1. Sources of Personal Data:

Web-Site Visitors' Personal Data is obtained in electronic form upon the entry of the visitors to ARCANOR's web-site.

4.6.2. Purpose of Processing

ARCANOR processes Web-site Visitors' Personal Data in order to provide the visitors with information they request, to contact with them to respond to their submitted comment or enquiry and to use essential cookies.

4.6.3. Length and Frequency of Processing:

Web-Site Visitors' Personal Data is processed until the reason of processing is fulfilled.

4.6.4. Data Minimisation:

ARCANOR obtains data from its Web-Site Visitors' upon the application of the visitors. Only the competent Personnels being in relation to their role and duties are allowed to have access to such data where they need to in order to perform their job functions.

Data is not used in manner incompatible with the purpose stated in Art 4.6.3.

5. BASIS OF PROCESSING

5.1. Regarding Mobile App Users' Personal Data

The legal ground for ARCANOR to process Mobile App Users' Personal Data is Consent. However, ARCANOR does not have any relationship with Data Subjects as it does not obtain

any direct Personal Data such as name, surname, e-mail address, telephone number or any kind of contact information from its Data Partners.

ARCANOR obtains data in the form of MAIDs, such as GAID, IDFA and IDFV, which are online identifiers used for personalized advertising collected through Mobile Applications in order to build marketing audiences and statistical insights.

All Data Partners are audited technically and in regulation through their Data Controller app store platforms. You can find further information in the following links:

- For IOS : https://www.apple.com/privacy/
- For Android : https://policies.google.com/privacy?hl=en

Privacy Notices are provided to the Mobile App Users by Data Partners.

ARCANOR makes the necessary due diligence in order to confirm that the data it obtains is in compliance with Data Protection Regulations. Within this scope, ARCANOR evaluates **i)** that the data it obtained from its Data Partners are collected under the legal basis of Consent from the Data Subjects, **ii)** that the Privacy Notices includes processing of Personal Data for advertisement purposes, transferring Personal Data to third parties, making Profiling and sending Personalized Advertisement and **iii)** that the Data Subject gives clear, opt-in consents to such processes.

ARCANOR requires all its Data Partners only to collect data in accordance with applicable laws and to ensure that proper information and choices are given to all Mobile App Users.

ARCANOR processes data only for advertising and statistical insights purposes and renders Services in forms of Anonymous Data such as statistics to its Customers. The outputs of its analysis are close to Re-identification by the Customers. Thus, outputs are not within the scope of Data Protection Regulations. On the other hand, the Customers undertake not to make any Re-identification efforts.

ARCANOR may upload segmented audiences directly to Marketing Platforms relying on its legitimate interest in order to perform its advertisement purposes whilst not overriding the fundamental rights of the Mobile App Users as Mobile App Users have consented to receive Personalized Advertisements. Upon written request, the list of Marketing Platforms can be shared.

In compliance with the relevant legislations, Marketing Platforms are entitled to send Personalized Advertisements only to those users who accepted to received such services.

5.2. Regarding Third Parties' Employees' Personal Data

The legal ground for ARCANOR to process Third Parties' Employees' Personal Data is legitimate interest as processing such data is necessary in order for ARCANOR to perform its Services in communicating with its Customers, Data Partners, Data Providers or other suppliers. Such processing does not override the rights of the Data Subjects as it includes only communicating purposes in line with the relationship between ARCANOR and the employer of the Data Subject. In addition, it is accepted that legitimate interest exists where there is a relevant and appropriate relationship between the Data Subject and Data Controller in situations such as where the data subject is a customer or service provider.

5.3. Regarding Personnels' Data

The legal grounds for ARCANOR to process Personnels' Personal Data are **i)** the necessity for the performance of the employment contract for Personal Data related day to day activities such as payroll, benefits and certain disciplinary issues and **ii)** legal obligations for Special Category of Data collected related to fulfilment of social security obligations of employers.

5.4. Regarding Web-Site Visitors' Personal Data

The legal ground for ARCANOR to process Web-Site Visitors' Personal Data is **t**he necessity for the performance of a contract or ARCANOR's legitimate interest.

Where Web-Site Visitor communicates with ARCANOR by making a request or inquiry, ARCANOR may rely on performance of a service contract in processing the information in order to best respond to the request or inquiry. ARCANOR may also process this data for its legitimate interest in using essential cookies.

6. BENEFITS

ARCANOR provides Data Fusion for the purpose of analysing sectors, markets and segments at a higher granularity, through the data enrichment from various alternative data sources, in order to enable data-driven strategies and marketing campaigns as well as strategic, operational and budget optimizations.

POI Data	Give Customers a reliable set of business and other locations to use in their own services. For instance, POI Data can be used to understand the points of interest on a map. Enables ARCANOR to determine the businesses and other locations that a device has visited.
Analysing Data	Enable Customers to target Personalized Advertisements and services based on inferred traits or preferences. For instance, a shop can use ARCANOR's Services to send exclusive offers to luxury clothes shoppers. Help Customers evaluate customer preferences and behaviours. Allow Customers to evaluate the effectiveness of advertising campaigns. For instance, a shopping mall could use Services to determine if its ad campaign persuaded Consumers to visit the mall. Provide Customers with insights and analysis of markets, Consumer behaviour and business opportunities, and enable Customer to draw their own insights and analysis. Give Customers a resource to design and improve other products and services. Allow Customers to optimize advertisement budgets, enhance corporate strategies through data-driven insights, increase productivity and efficiency and gain considerable competitive edge within the market.

7. RISKS

Low potential of cybersecurity risks arisen from possible cloud provider OS and software vulnerabilities independent from software, security updates and patches which has minimal impact of data leakage mitigated through acceptable measures of software updates and security procedures.

Cybersecurity risk which may occur through an undisclosed vulnerability causing a spoofed/malicious email.

8. STORING PERSONAL DATA

ARCANOR stores the data it holds in its cloud solution. Therefore, it transfers data to its cloud service provider who acts as Data Processor. ARCANOR makes the necessary due diligence regarding the implementation of appropriate organizational and technical security measures to protect data against unauthorized disclosure. The cloud service provider has a security assurance program that uses best practices for global privacy and data protection to operate securely, and to make the best use of a security control environment. These security protections and control processes are independently validated by multiple third-party independent assessments. It complies with ISO 27018, a code of practice that focuses on protection of personal data in the cloud and provides the technical capability to ensure ARCANOR can satisfy data portability right of Data Subjects. The cloud service provider ensures that data remain within the controllership of ARCANOR.

ARCANOR also stores e-mails in its e-mail provider who also acts as Data Processor. ARCANOR makes the necessary due diligence regarding the implementation of appropriate organizational and technical security measures to protect data against unauthorized disclosure.

Web-site Visitors' Personal Data is stored in the web platform provider in order the web-site to function properly using essential cookies.

9. TRANSFER OF PERSONAL DATA TO THIRD PARTIES

9.1. Transfer to Customers

ARCANOR fuses the data it obtains from its Data Providers in order to build audience segments through machine learning, statistical analysis, clusters and serve this to its Customers as a Service. Therefore, Mobile App Users' Personal Data is not disclosed to Customers, only anonymized statistics and insights are shared with Customers which are not included under Data Protection Regulations.

9.2. Transfer of Third Parties' Employees' and Personnels' Personal Data

Third Parties' Employees' Data and Personnels' Data can be disclosed to third parties within the scope of legitimate interest of ARCANOR, fulfilment of a contract and/or compliance with its legal obligations provided that the disclosure shall be limited with its purpose and that having implemented the appropriate organizational and technical security measures to protect data.

9.3. Transfer to Marketing Platforms

ARCANOR uploads segmented audiences to Customer's Marketing Platforms, -especially to social media networks' whose only working field is to make Personalized Advertisements, in order to accomplish its advertisement purpose, being within the scope of ARCANOR's legitimate interest. ARCANOR, removes the segmented audiences from the Marketing Platforms at the end of its Services.

9.4. Sharing Data with Government, Law Enforcement, Or Regulatory Bodies

ARCANOR may disclose data in cases it believes that such action is necessary to comply or assist with applicable laws or regulatory investigations, or to respond to a court order, judicial or other government subpoena, warrant, or law enforcement request. ARCANOR shall share the data limited with the formal request.

10. SECURITY OF PROCESSING

ARCANOR takes data privacy very seriously and is committed to protect Data Subjects' Personal Data. It has implemented appropriate technical, organisational, and physical measures to prevent Personal Data from being accidentally lost, used or accessed in an unauthorised way, altered, or disclosed. It takes the necessary precautions in order to prevent Data Incidents. In addition, it limits internal access to Personal Data by Personnels or other third parties. They process Personal Data on ARCANOR's instructions on need-to-know basis, and they are subject to a duty of confidentiality.

The security measures are as the followings:

- Training, communication and awareness
- Password protection, 2-FA user authentication where available, encryption, firewalls, anti-virus and use of encrypted communications
- Access, usage, network log controls, monitoring and notifications
- Administration of security privileges through access roles, cloud policies and user groups
- Scanning of documents for anti-malware
- Internal cybersecurity audits on security of internal systems
- Following and implementing updates and security patches on operating systems, Applications and/or Infrastructures

ARCANOR uses de-identification of data, arrangements or destruction of data upon request or were unneeded, back-up and/or deletion of data, quarterly audit for internal compliance, password protection, encryption, anonymization and pseudonymisation as mechanisms to protect Personal Data.

ARCANOR renders Services in forms of Anonymous Data to its Customers by providing location-based statistical insights and marketing segments which anonymizes the activity of any specific individual and prevent any specific Re-identification.

With the acknowledgement of this Policy, the Customer agrees and undertakes not to initiate any Re-identification effort and use ARCANOR's Services outside the scope of its purpose.

11. DATA QUALITY

ARCANOR checks that data sets are comprehensive, complete, without bias, accurate in order to comply with the data minimization principle. ARCANOR ensures that the Consents of the Mobile App Users are up-to-date.

12. INDIVIDUAL RIGHTS

In cases the Data Subject is located in the EU/EEA/UK or Turkey, Data Protection Regulations list the following rights:

- The right to be informed
- The right of access by requesting access to it
- The right of rectification of incorrect data
- The right to erasure by asking for it to be erased (the "right to be forgotten")
- The right to restrict processing
- The right to data portability by asking for a copy to take to another service provider
- The right to object to its processing
- The right not to be subject to automated decision-making
- Right to withdraw Consent, including transfers, Automated Processing, Profiling

Data Subjects may apply the above-mentioned rights through the Data Partners.

As ARCANOR obtains data through Mobile Applications, once Data Partner exercises a Data Subject request, ARCANOR's records are updated accordingly.

In cases where Data Subjects withdraw their consents, ARCANOR receives a notice from its Data Partner and it acts immediately by making the relevant data unidentifiable.

As ARCANOR does not process contact or identification data such as names or emails, it may not know whether or not it is processing any data relating to the applicant, and may not always be able to meet specific requests. However, ARCANOR assures Data Subjects that it will always use reasonable efforts to do so.

In case of any issue, please contact ARCANOR using the details in this Policy. In cases where Data Subjects believe that ARCANOR has not respected their rights, they also have a right to make a complaint to the Supervisory Authority in their country.

13. REPORTING A BREACH

ARCANOR maintains security incident management procedures and notifies its Customers without undue delay in case it becomes aware of a Data Incident occurred due to an accidental or unlawful destruction, loss, alteration or unauthorized disclosure within 72 hours.

ARCANOR ensures that it makes reasonable efforts to identify the cause of such Data Incident and takes those steps as ARCANOR deems necessary and reasonable in order to mitigate the cause of such a Data Incident to the extent the mitigation is within ARCANOR's reasonable control. The obligations herein shall not apply to incidents that are caused by Customers.

14. RETENTION AND DISPOSAL

ARCANOR does not store Personal Data for longer than necessary to fulfil its purposes including for the purposes of satisfying any legal, regulatory, tax, accounting, or reporting requirements. ARCANOR may however, retain data for a longer period as reasonably necessary for it to deal with a complaint or if it reasonably believes that litigation may be likely with respect to the relationship.

14.1. Retention Periods

TYPE	STORING PERIOD	RETENTION PERIOD
MOBILE APP USERS	During the performance of the Service and 60 (sixty) months after the purpose of processing is fulfilled.	60 (sixty) days after the purpose of processing is fulfilled
THIRD PARTYS' EMPLOYEES	Until the purpose of processing is fulfilled.	60 (sixty) days after the purpose of processing is fulfilled
PERSONNELS	During the relevant employment contract and 10 (ten) years after its termination	60 (sixty) days after the purpose of processing is fulfilled
WEB-SITE VISITOR	Until the purpose of processing is fulfilled.	60 (sixty) days after the purpose of processing is fulfilled

14.2. Retention Method

After the fulfilment of purpose all types of data is corrupted and anonymized through one-way hashing methods then stored as archives or completely deleted including all backups.

14.3. Back-up

Frequent backups are taken for Mobile App Users' and Personnels' Personal Data in cloud service provider, while Third Parties' Employees and Web-Site Visitors' are taken on the e-mail provider.

14.4. System Decommissioning

Systems that require termination is completely destructed within the cloud service provider, which does not require migration.

15. ACCOUNTABILITY

ARCANOR keeps all the necessary records in order to demonstrate that it complies with Data Protection Regulations.

Upon Customer's request, ARCANOR may provide Customer with reasonable cooperation and assistance needed to fulfil Customer's obligation under the Data Protection Regulations to carry out a data protection impact assessment related to Customer's use of the Services, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to ARCANOR.

16. TRAINING AND AUDIT

ARCANOR ensures that its employees have received appropriate training on their responsibilities regarding the protection of Personal Data. ARCANOR ensures that its Personnel engaged in the processing data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities and have executed written confidentiality agreements. ARCANOR ensures that such confidentiality obligations survive after the termination of the personnel engagement.

ARCANOR realises periodic internal audits every 3 (three) months in order to ensure processes are in compliance with security measures expected from its operations.

17. AMENDMENTS

This Policy may be updated from time to time as ARCANOR's Services evolve and to keep pace with technical or legal requirements.

ARCANOR shall make Data Subjects aware of such changes in the form of a clear and prominent notice on ARCANOR's website.

18. CONTACT

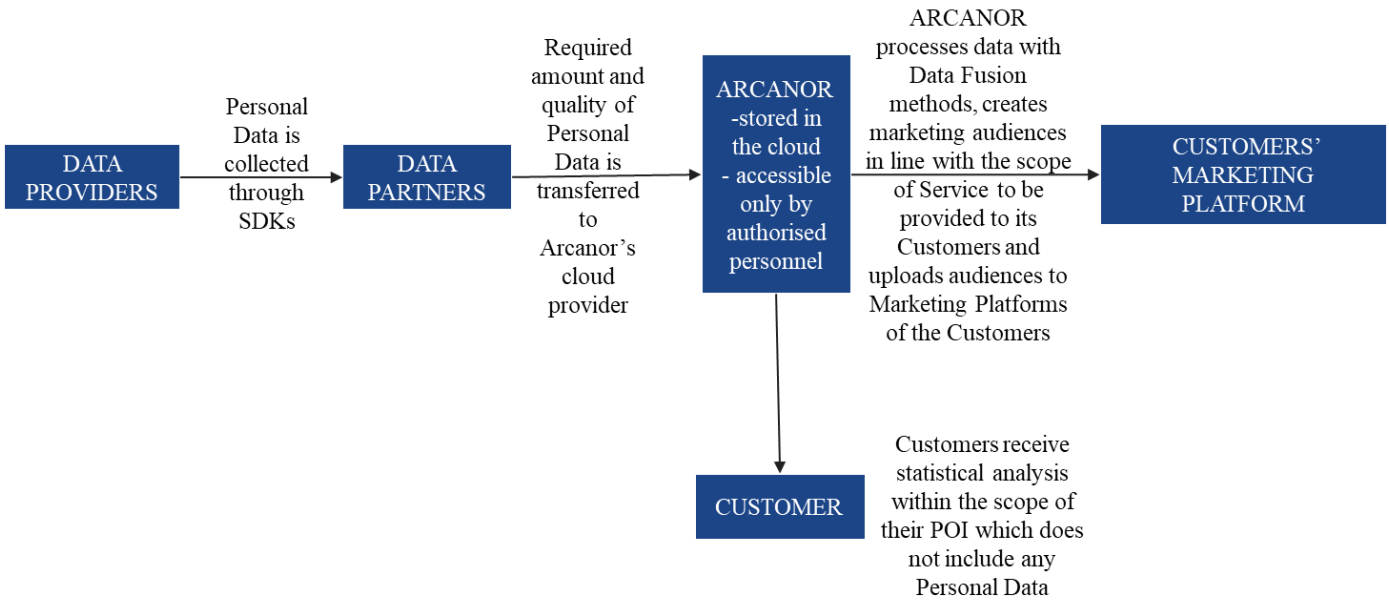
Any inquiry regarding this Policy or other data privacy issues please contact:

legal@arcanor.com

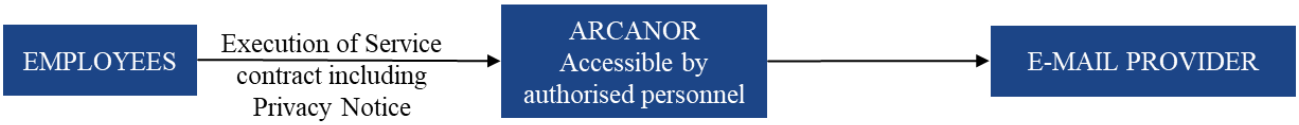
ANNEX-1 : DATA FLOW MAPS

	Type of Personal Data	Lawful Basis	Purpose
MOBILE APP USERS	POI data, mobility, geographical location, internet usage data, online identifiers (IP, MAIDs), Mobile Apps' data (latitude, longitude, areas of interest), GPS data, navigation data (vehicle, traffic speed, destination), socio-economic data, Sectoral data (ADS-B, AIS, electricity consumption), Meta data (market prices, social media and Location)	Consent in making Data Fusion / Legitimate interest in uploading to Marketing Platforms	Statistical analysis and create marketing audiences
THIRD PARTYS' EMPLOYEES	name, surname, ID number, e-mail address, telephone number, authorized signatures lists, billing information	Legitimate interest	Fulfilment of the service contract
PERSONNELS	national id card, address, telephone number, passport, CV, diplomas, certificates, bank account details, blood type, medical certificate	Performance of a contract	Execution and fulfilment of the employment contract
WEB-SITE VISITORS	name, surname and e-mail address, cookie ID	Performance of a contract and legitimate interest	Communication for inquiries and usage of essential cookies.

MOBILE APP USERS' PERSONAL DATA



THIRD PARTIES' EMPLOYEES' PERSONAL DATA



PERSONNELS PERSONAL DATA

WEB-SITE VISITORS' PERSONAL DATA