LIVE! PROMOTERS

DATA PROTECTION POLICY

{25.5.2018}

{ Live Promoters Oy – Business ID: 2176771-0}

Contents

1. DATA PROTECTION POLICY 5

1.1. DEFINITIONS 5

1.2. ROLES 5

1.3. DATA PROTECTION OFFICER 5

1.4. RECORD OF PROCESSING ACTIVITIES 5

1.5. SPECIFIC DATA ITEMS TO BE STORED AND PROCESSED 6

1.6. HOW DATA WILL BE OBTAINED 6

1.7. DATA TRANSER SAFEGUARDS 6

1.8. HOW DATA WILL BE PROCESSED 6

1.9. RETENTION TIME OF DATA 7

1.10. HOW DATA WILL BE STORED 7

1.11. PROCESSING LOCATIONS 7

1.12. CALL RECORDINGS 7

1.13. WHERE DATA MAY BE TRANSFERRED AND UNDER WHAT CIRCUMSTANCES 7

1.14. WHO WILL HAVE ACCESS TO DATA AND HOW 7

2. COMPLIANCE WITH INDIVIDUALS RIGHTS 9

2.1. GENERAL 9

2.2. RIGHT TO ACCESS 9

2.3. RIGHT TO RECTIFICATION 9

2.4. RIGHT TO ERASURE (RIGHT TO BE FORGOTTEN) 9

2.5. RIGHT TO RESTRICT PROCESSING 9

2.6. RIGHT TO DATA PORTABILITY 9

2.7. SECURITY OF PROCESSING 9

2.8. NOTIFICATION OF PERSONAL DATA BREACH 10

2.9. COMMUNICATION OF PERSONAL DATA BREACH TO DATA SUBJECT 10

2.10. TRAINING 10

2.11. CERTIFICATIONS 10

3. RISKS ASSESSMENT MODEL.....11

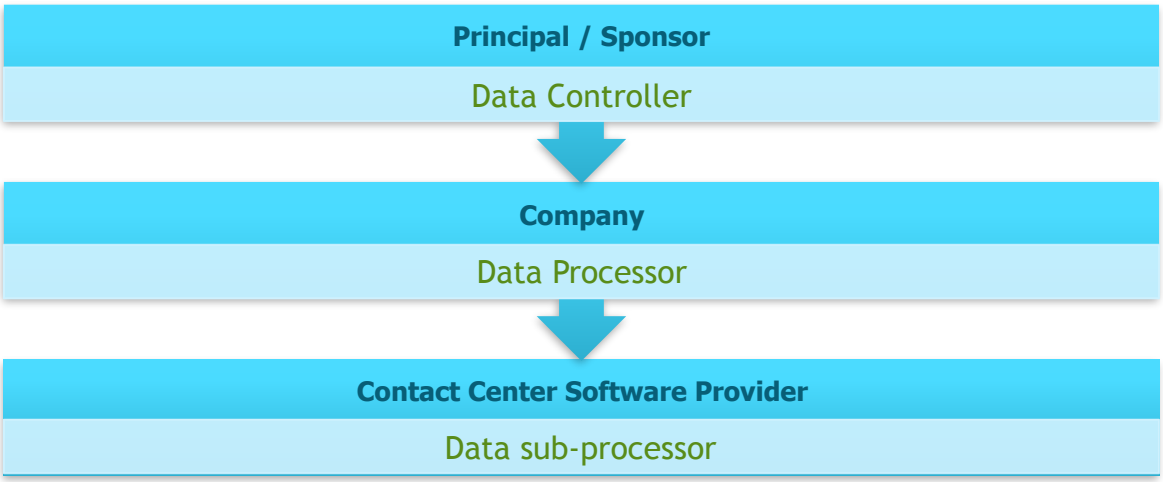
1. Data Protection Policy

1.1. DEFINITIONS

Personal Data: In the context of GDPR personal data is defined as information relating to an identified or identifiable natural person, data subject. An identifiable 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 one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

Principal: A Principal or Sponsor is the entity for whom the Company does outsourced direct marketing.

1.2. ROLES



1.3. DATA PROTECTION OFFICER

The company does not meet any of the criteria that would require electing a Data Protection Officer under Article 37:

- Public authorities
- Companies who process data requiring 'regular and systematic monitoring of data subjects on a large scale'.
- Companies who process any special category of personal data, such as political opinions, religious beliefs or ethnic origins.
- Companies who process personal data relating to criminal convictions or offences.

The company has named a primary contact person regarding data protection related enquiries: **Rasmus Lindroos**

1.4. RECORD OF PROCESSING ACTIVITIES

Categories of data being processed are Employee registry, Records relating to contact center work, Customer support activities and Direct marketing, data on these activities is stored in the Contact Center software. The contracts with Principals, together with their contact details, are stored at: Live Promoters Oy, Eteläesplanadi 22 C 28, 00130 HELSINKI, FINLAND

Together this forms the Record of Processing activities as per Article 30 of GDPR.

1.5. SPECIFIC DATA ITEMS TO BE STORED AND PROCESSED

The following data classes will be stored and processed:

1. Data relating to Customers and Prospects for the purpose of customer service and direct marketing:
    - First name
    - Last name
    - Phone number
    - Address
    - Email address
    - Transaction and Order history
    - [other]

2. Data relating to transactions with Customers and Prospects:
    - Contact method
    - Related contact
    - Time stamps of the contact
    - Outcomes

3. Data relating to Blacklisted Customers and Prospects:
    - Phone number
    - Address

1.6. HOW DATA WILL BE OBTAINED

Data on Customers and Prospects will be obtained from:

- Third party data providers
- Live Promoters Oy marketing registry

1.7. DATA TRANSER SAFEGUARDS

All data involving personal information, such as data exchanged between Third party lead providers and Principals, will be done through:

Secure encrypted portal inside the Contact Center Software LEADDESK

Encrypted email

Encrypted FTP-Server

1.8. HOW DATA WILL BE PROCESSED

The data will be processed within the Contact Center Software to enable customer service and direct marketing operations and to provide Contact Center agents visibility to Customers and Prospects, as well as enable Contact Center managers to efficiently run their day to day Contact Center operations according to normal industry practices.

1.9. RETENTION TIME OF DATA

To comply with local regulation relating to employment disagreements and the fulfillment of contracts with Principals, data relating to Customers and Prospects will be retained for the duration of 4 years.

1.10. HOW DATA WILL BE STORED

Data relating to Customers and Prospects will be stored securely inside the Company's Contact Center Software. In case there are any data outside the software (such as local exports) these are maintained and removed according to the same principles.

1.11. PROCESSING LOCATIONS

Data will be processed at the company's physical location, at Eteläesplanadi 22 C 28, 00130 Helsinki, Finland. Data processing inside the Contact Center Software is always done within the European Economic Area. The list of current data processing locations, as applicable from time to time, is available upon request from the Contact Center Software provider.

1.12. CALL RECORDINGS

Call recordings are treated according to industry best practices as defined by local direct marketing associations, such as:

- Finnish ASML: www.asml.fi
- Swedish Kontakta: www.kontakta.se
- Norwegian Nordma: www.nordma.no
- German CCV: www.callcenter-verband.de
- KSF: www.klantenservicefederatie.nl

1.13. WHERE DATA MAY BE TRANSFERRED AND UNDER WHAT CIRCUMSTANCES

Data may be transferred to Principals to fulfill contractual requirements. The company should not be responsible for handling consumer requests and should never send information directly to anyone else than the principle. All requests that are not made by the principal, should be forwarded to the principal, who is responsible for further actions.

1.14. WHO WILL HAVE ACCESS TO DATA AND HOW

The Contact Center Software is used to define appropriate user and data access levels on per group and user basis. In principle there are four levels of users:

- Agents
    - Agents have access to individual Customers or Prospects data on per need bases, as well as historical data on Customers and Prospects they are pursuing. They can also view and audit their own usage data of the Contact Center Software.
- Team leaders
    - Team leaders have access to usage data of agents in their Team, as well as Customer and Prospect data inside of projects. Some access (e.g. Prospect and Customer data) may be limited.
- Managers

- Managers have access to all teams' User, Customer and Prospect data. The extent of the access may be limited according to data type, similar to Team leaders.

- Administrators
    - Administrators have full access to the whole system and their access cannot be limited.

2. Compliance with Individuals Rights

2.1. GENERAL

As the company is only a data processor on behalf of the principle, all requests from data subject will be redirected to the appropriate principle.

The company can receive requests from principles through the following channels:

- Email to palaute@livepromoters.fi
- Phone call to support +358447866672

Any request not directed through these channels must be redirected to the appropriate channel in order to ensure the right of the data subjects.

2.2. RIGHT TO ACCESS

All data of Customers and Prospects is stored solely inside the Contact Center Software, which provides the means to export data based on identification by:

- Phone number
- Email address
- Social security number

2.3. RIGHT TO RECTIFICATION

As the Company works solely as a data processor on behalf of the Principal, all requests to rectify data will be forwarded to the Principal in question. The Company has the necessary means to support the Principal in rectifying the data being processed inside the Company's Contact Center Software.

2.4. RIGHT TO ERASURE (RIGHT TO BE FORGOTTEN)

As the Company works solely as a data processor on behalf of the Principal, all requests to erase data will be forwarded to the Principal in question. The Company has the necessary means to support the Principal in erasing data being processed inside the Company's Contact Center Software in a way that also supports keeping data for which there is a legitimate reason.

2.5. RIGHT TO RESTRICT PROCESSING

As the Company works solely as a data processor on behalf of the Principal, all requests to restrict data will be forwarded to the Principal in question. The Company has the necessary means to support the Principal in restricting the data being processed inside the Company's Contact Center Software.

In case a request to restrict the processing of data is received, the Contact will be immediately blacklisted as a safety precaution, thereby restricting processing on the Company side.

2.6. RIGHT TO DATA PORTABILITY

The Contact Center Software in use enables the export of all data in CSV format, which is widely supported for data transfer.

2.7. SECURITY OF PROCESSING

Processing of data is secured by the following means:

1. Contact Center Software user controls and access levels are used to prevent any unauthorized access, reading, copying, removal or alteration of data.
2. All data stored inside the Contact Center Software is physically secured using SOC3 and ISO27001 certification. All data handled outside of the Contact Center Software is encrypted.
3. Connection to Contact Center Software is secured using SSL-technology.
4. An Audit trail of personal data transmission is handled onsite using physical audit logs. Inside the Contact Center Software an audit log is automatically generated and stored and is accessible upon request from the Contact Center Software provider.
5. In order to ensure that data processing on behalf of the Data Controller is only done in the manner prescribed, access is only given on per need bases, and all personnel with access to data are trained on the agreed process.

2.8. NOTIFICATION OF PERSONAL DATA BREACH

As the Company acts only as a data handler towards the Principals, the Company will support the Principals in cases of data breaches according to the process agreed to in the DPA.

2.9. COMMUNICATION OF PERSONAL DATA BREACH TO DATA SUBJECT

As the Company acts only as a data handler towards the Principals, the Company will support the Principals in cases of data breaches according to the process agreed to in the DPA.

2.10. TRAINING

As part of on-boarding and ongoing employee training programs, employees will be trained on secure data handling, confidentiality requirements and GDPR.

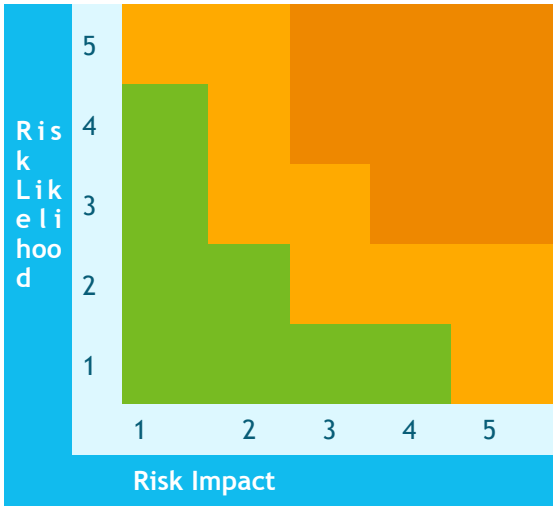
2.11. CERTIFICATIONS

The Company follows the development of certifications for GDPR compliance and should new business goals become available, the Company will strive to adopt them.

In choosing data processing partners, such as a Contact Center Software provider, the Company considers only suppliers that meet verified high security standards, such as up-to-date ISO27001 and SOC3 certification.

3. Risks Assessment Model

The Company has conducted an internal risk assessment. The risk assessment is based on identifying risks and then assessing them on two vectors: likelihood and impact. These two factors form a Risk score using the following table:



Example assessment:

Description	Likelihood	Impact	Prevention
Person represents another personality to get their data	2	3	Requirement for valid ID.
Person claims to own email that he / she doesn't own	2	3	With personal emails that are not attached to any official person or organisation, the only way to confirm them is to send an email to that address. However, this only proves that person has access to email, so there is no 100% mitigation available.
Data provided by Principal does not meet GDPR requirements	2	4	A Data Processing Agreement will be made with each Principal.
Principals and Third-parties send contact data over unsecure channels	4	4	All Principals are instructed to transfer data through a secure portal inside the Contact Center Software.
Employee breach of NDA	2	4	All employees are trained on their responsibilities regarding non-disclosure.