iReachm.com GDPR Compliancy Document

1. Accountability

1.1 Has iReachm.com appointed a data protection officer?

1.1.1 Yes, iReachm.com does indeed employ a person appointed for this purpose. This person is responsible for securing all data that arrives and leaves at iReachm.com.

1.2 Does iReachm.com keep a processing register?

1.2.1 Yes, iReachm.com keeps a processing register.

1.3 Does iReachm.com have a data breach notification plan?

1.3.1 Yes, iReachm.com has such a plan.

1.4 How does iReachm.com ensure that privacy of the data is implemented in the organization in itself?

1.4.1 iReachm.com has received a VLAIO grant specifically used for implementing privacy by design in the organization. Various initiatives were taken, including data encryption, validation, ...

1.5 How does iReachm.com ensure privacy in the internal programs in itself?

1.5.1 iReachm.com has ensured that the internal programs are only accessible with local IP addresses and all data is encrypted.

1.6 Does iReachm.com require users to process the data?

1.6.1 iReachm.com has included this in the privacy statement / general conditions. The iReachm.com app will always request permission to retrieve certain data. The user always has the possibility to respond negatively to this, and subsequently iReachm.com will not use the blocked data by the user.

2. Customer rights

iReachm.com is always accessible via chat, mail or telephone to give users the possibility to request the following information. iReachm.com will always release the following information if necessary;

2.1.1 Information available from the user and the uses
2.1.2 Information about the data access
2.1.3 The right to rectify certain information
2.1.4 The right to reassurance with regard to the information supplied by the user
2.1.5 The right to restrictions regarding the processing of the data made available by the user
2.1.6 iReachm.com is obliged to give notification to the user for each action. The user can decide for himself whether it is via mail or via mobile
2.1.7 Information regarding data transfer. This information can be supplied in JSON format.
2.1.8 The right to object or protest.
2.1.9 The right to object against automated individual decision-making

3. Organizational measures

3.1 Does iReachm.com follow an industrially accepted standard such as ISO27001?

3.1.1 iReachm.com does not use a standard within this framework. In other words, iReachm.com is not certified for ISO, COPC, ...

3.2 Does iReachm.com as an organization have a policy with regard to limiting access to sensitive data for both employees and contractors?

3.2.1 iReachm.com has such a policy where the following initiatives have been taken:

- A limited number of people within the company have been granted rights to be able to access certain information by means of limited SSH access.
- Access to data is only granted on subsets of the total datasets and is managed in different database environments.

3.3 Does iReachm.com have a policy where it is checked on a regular basis whether there are certain employees or contractors who no longer need access to certain items?

3.3.1 iReachm.com has a policy where every month all passwords are changed and users are asked to choose a new password. If certain employees or contractors no longer work in or for iReachm, they no longer have access to the data.

3.4 Does iReachm.com have a policy that takes into account the inspection or use of under contracting or third parties?

3.4.1 iReachm.com establishes so-called Data Subprocessor agreements for each party with whom they cooperate

3.5 Has iReachm.com as an organization concluded a confidentiality document and / or data security agreements with its employees and contractors?

3.5.1 iReachm.com has this documentation and this is signed by both parties as standard with every new colleague / contractor.

3.6 Does iReachm.com provide an obligatory training on security as an organization?

3.6.1 No explicit training is provided, but the work regulations contain the necessary guidelines in this respect

3.7 Does iReachm.com as an organization have a policy for disciplining personnel when they violate the data security processes & procedures?

3.7.1 iReachm.com does not have such a policy.

3.8 Does iReachm.com have a clean desk policy?

3.8.1 iReachm.com has internally a clean desk policy for its employees within the office.

3.9 Are there security measures for the physical location (s) where the information is treated.

3.9.1 iReachm.com works together with Nucleus as a data center. For further questions about the data center, please refer to Nucleus. To enter the iReachm.com office, badges are provided for each employee to enter the office. Specifically, an employee needs both a badge and a key to enter the office.

4. Technical measures

4.1 Does iReachm.com provide encryption when sending personal information?

4.1.1 All communication of such information is protected by SSL encryption, never an unencrypted communication will be sent.

4.2 Does iReachm.com provide encryption of personal information in general?

4.2.1 iReachm.com ensures that every password Sha256 is encrypted.

4.3 Does iReachm.com use firewalls to secure sensitive information?

4.3.1 The hosting partner of iReachm.com, Nucleus, provides very strict security including the use of firewalls.

4.4 Does iReachm.com provide regular updates of the computers / servers & technical infrastructure?

4.4.1 Nucleus takes care of all updates for us on a regular basis. If it concerns an urgent update, they also execute this immediately.

4.5 Does iReachm.com use the most current anti-virus & anti-spyware?

4.5.1 Nucleus provides Trend Micro malware protection which allows malicious software to stop before it reaches the servers. For the time being, iReachm.com does not have this software.

4.6 Are our internal programs designed in such a way that they contain rules about complex passwords?

4.6.1 iReachm.com uses software applications that each have regulations concerning the complexity of a password (length, complexity, history, etc ..)

4.7 **Does iReachm.com use a secure environment to write software code such as CERT, OWASP?**

4.7.1 iReachm.com uses the Meteor platform as a framework. For more information, please visit; https://guide.meteor.com/security.html

4.8 Does iReachm.com have the possibility to generate audit logs to check who has access to which resources at a certain time?

4.8.1 1.1.1 iReachm.com has access to this as well as an API audit logging.

4.9 Has iReachm.com already experienced security breaches in the last 5 years?

4.9.1 iReachm.com has not experienced any security breaches in the past 5 years.

4.10 Does iReachm.com provide backups of all information as an organization?

4.10.1 iReachm.com indeed provides back-ups of all available information. Each Nucleus server automatically provides a 7-day backup system by default. Back-ups are made every day by taking a storage snapshot and storing it at another data center. In the case of iReachm.com, these servers are hosted in Antwerp. The backups are kept in a data center in Brussels.

4.11 Does iReachm.com use a third paty for independent check-up regarding the security systems and their effectiveness?

4.11.1 iReachm.com does not appeal to an external party for these checks.

4.12 Does iReachm.com make information anonymous on non-production environments?

4.12.1 iReachm.com manages the data of people in different database environments so that no connections can be made between the various data sources due to the limited subset access of the employees and customers to these data.

5. 1 3rd party risk

4.13 Is all data stored in the EEA?

4.13.1 iReachm.com works together with Nucleus for this. Nucleus works with 4 data centers in Belgium; Antwerp, Nossegem, Diegem & Zaventem. Both the datacenter in Nossegem & Antwerp are completely built up as high density data centers. The datacenter in Diegem is provided as a network datacenter where we connect our fiber network to different uplink providers.

4.13.2 Nucleus in turn provides for the following initiatives within the framework of GDPR:

4.13.2..1 Nucleus has a dual role: that of data processor (for the data of your customers that you place with us) and that of data processing officer (for your personal data as a customer of Nucleus).

4.13.2..2 As a data processor, we provide the data that you have collected as data processing manager. In that role we ensure that

- it is clear who bears legal responsibility. Depending on the type of service, we as a processor carry more or less responsibility.
- every employee is perfectly aware of all that GDPR implies
- your data is maximally secured (thanks to our ISO 27001 certificate for data security)
- we keep logs of data processing that we do on your data
- a possible violation of the security measures on our managed infrastructure is reported to you as soon as possible
- we closely monitor the efforts of our suppliers and partners to become GDPR-compliant
- you get secure access to your data or we provide you with a copy of it when you choose a different data processor as your client

4.13.2..3 As data processing officer we manage your own personal information (as a customer of Nucleus). We ensure that we are also GDPR-compliant in this role. That means that you as a data subject have a number of rights.

- You may view your data and have them corrected if necessary
- You may change your mail preferences or withdraw your active consent at any time. You can do that here.
- You may request information about your data (how long we keep your data, why we collect that data, which persons / organizations have access to it, etc.).
- You may ask for your data to be deleted. This concerns data for which active consent has been given or when there is a legitimate interest. Dates that are required for contract related reasons (to be able to send invoices or to report certain technical adjustments, for example), are subject to statutory retention periods. After these terms, the data will be deleted automatically.