General Data Protection Regulation

Legal Service Agreement Crobox

Leonard Wolters, Revision 0.5, October 2017

Table of Contents

Terms & Definitions

1. **Data Controller** - The entity that determines the purposes, conditions and means of the processing of personal data. Generally this sums down to the Party that holds and owns the Data, hereinafter referred to as Client
2. **Client** - See Controller
3. **Crobox** - The Data Processor as well as the Service Supplier
4. **Data Processor** - The entity that processes (personal) data on behalf of the controller. In more general terms, the Party that processes the data, which is Crobox
5. **Service** - The services provided by Crobox, to be summarized as ‘Persuasion-as-a-Service’.
6. **Supplier** - The supplier of the services described in this document, which is Crobox
7. **Service Agreement** - A document or contract holding all Services offered to Client
8. **Party** - All parties to this Service Agreement; hereinafter collectively also referred to as the "Parties" and individually as a "Party"
9. **Data Subject** - The ‘owner’ of the data, in our context often designated by a natural person
10. **UUID** - A Unique User IDentifier. An unique sequence of 40 randomly picked characters & numbers used to identify Data Subjects
11. **Personal Data** - Any information related to a Data Subject that can be used to directly or indirectly identify that Data Subject. Examples: UUID, name, email address, IP address
12. **Sensitive Data** - A special category of Personal Data to which additional protections apply. These categories include revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health or sex life related
13. **Profiling** - Any means 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 personal preferences
14. **Pseudonymisation** - Processing of personal data in such a manner that the personal data can no longer be attributed to a s specific data subject without the use of additional information

1 Introduction

As from May 2018 the General Data Protection Regulation (GDPR) will be enforced resulting in stringent regulations concerning the processing and protection of personal data. This document contains all information about Crobox and these upcoming regulations.

This document starts with focussing on the regulations that are applicable to Crobox. Following is a separate chapter about organisational and technical measures installed to meet the high protection levels and standards required by the GDPR.

Afterwards a full chapter is dedicated to Data Governance -both Client as Data Subject oriented- which forms an essential part of the GDPR. This chapter also presents out-of-the-box solutions provided to Clients and their customers required in order to comply to all regulations. This documents ends by providing some relevant information about Crobox including disclaimers and contact information.

To summarize; this document should provide you with a clear understanding of all GDPR related matters and what Crobox has done in order to comply to them. Where possible we refer to specific articles found in the GDPR.

> It is highly recommended to read the document entitled ‘Personal Data’ in advance. This document provides detailed information about Crobox’ Data Processing and all Personal Data processed.
>
> This document can be downloaded free-of-charge. See 5.1 Downloadable documents

1.1 Document history

0.5	2017-10-31	Changed title and several small corrections
0.4	2017-10-17	Moving cookie policy to separate document and proof reading.
0.3	2017-10-05	Moving information to Personal Data document and cleaning up
0.2	2017-09-28	Fact Checking all Articles
0.1	2017-09-14	Initial document

2 General Data Protection Regulations

2.1 Data Processor

Crobox qualifies as a Data Processor and should therefore comply to at least all regulations concerning Data Processors.

2.2 Service Agreement (Article 28)

Attached to this document there is a Service Agreement Template that forms an integral part with all commercial & legal contracts in place between Crobox and Client, see Appendix: Service Agreement Template

2.3 Explicit Instructions (Article 29)

Crobox requires the **explicit and written instructions** of the Client for any Data Processing, unless required to do so by Union or Member State Law. Without these instructions Crobox won't offer its Services and can't be held responsible for any claim and/or damage. This requirement is enforced in the Service Agreement Template found as appendix in this document

2.4 Client Supervisory Powers

The Client is not only entitled but even encouraged by Crobox to carry out inspections either by themselves or any other approved external auditor, for the sole purpose to convince itself of the compliance with this Service Agreement in business operations. These inspections should primarily target the verification of 4. Technical and Organisational Measures.

Such inspections should be communicated to Crobox in advance in written form (e.g. email), taken into account a two week notice. Crobox ensures that Client is able to verify compliance with the obligations as set out in Article 28 GPDR.

These inspections should align and not impact Crobox general way of working

2.5 Personal Data Breach (Article 33 & 34)

Crobox complies with the obligations concerning the security of personal data, reporting requirements for data breaches, data protection impact assessments and prior consultations, referred to in Articles 32 to 36 by the installment of the following measures and precautions:

Whenever Crobox detects or suspects a (personal) data breach it will notify Client not later than 72 hours after such detection or suspicion. Each notification will be accompanied with:

1. The nature of the data breach,
2. Contact details of the Data Protection Officer,
3. Consequences (if any) of the data breach, and
4. Measures to be taken to mitigate

Crobox can't inform Data Subjects about any (possible) Personal Data breach since **we don't store any contact information** other than the UUID. Hence, without having physical or online addresses (e.g. email) we simply can't contact the Data Subjects directly (Article 34)

Crobox ensures an appropriate level of (data) protection through 4. Technical and Organisation Measures. Next to that, Crobox offers Client full support with regard to prior consultation of any supervisory authority.

2.6 Data Protection Officer (Article 37, 38, 39)

Crobox has a designated Data Protection Officer that fully complies to Articles 37 to 39. You can find contact details at: 7.3 Data Protection Officer.

Crobox' Data Protection Officer is involved in all issues and measures which relate to security and is even aware of all software designs and implementations. The Data Protection Officer has direct access to the code base and can perform independent checks and verifications.

Next to a designated Data Protection Officer you can also find contact details of our Chief Security Officer, which can provide all ins and outs about our (technical) security measures.

2.7 Codes of Conduct (Article 40, 41)

Not available at the moment. To be expected around Q1 2018.

2.8 Certification (Article 42, 43)

List of the following certifications:

1. Our infrastructure / hosting is ISO 27001, ISO 9001, PCI-DSS, NEN 7510 and ISAE 3402 certified.

2.9 Transfers of personal data (Article 44, 45)

Crobox is headquartered in Amsterdam, the Netherlands. We're registered under the Dutch Law and are not considered -nor make part of- an international organisation. Therefore we don't need to apply to the regulations as set forth in Chapter V.

Crobox ensures that its processing of data is carried out exclusively within a Member State of the European Union (EU) or within a Member State of the European Economic Area (EEA). Each and every Transfer of Data to a State which is not a Member State of either the EU or the EEA requires the prior agreement of the Client and shall only occur if the specific Conditions of Article 44 et seq. GDPR have been fulfilled.

Chapter V of GDPR clearly states that when international organisations are involved the regulations of Chapter V apply. In order to comply to these regulations Crobox requires a waiver (embedded in the Service Agreement Template) ensuring that Client -only when considered an international organisation- ensures adequate levels of (data) protection (Article 45).

3 Technical and Organisational Measures

Crobox has installed numerous technical and organisational measures in order to ensure an appropriate level of (data) protection. These measures in particular:

1. Take into account the circumstances and purposes of the processing as well as the projected probability and severity of a possible infringement of the law as a result of security vulnerabilities, and
2. Enable an immediate detection of relevant infringements events.

3.1 Privacy By Design and by Default (Article 25)

Crobox considers data privacy on the onset of all projects, products, product development and Services offered; not as an afterthought. Crobox' Data Protection Officer is involved in all issues, measures and (software) designs which relate to security and has independent & direct access to all source code.

3.2 Technical Measures

Technical measures are divided into various subsections, each of them separately discussed.

3.2.1 Security

1. Employee related:
    a. All workstations (laptops & desktops) of employees are encrypted using disk encryption
    b. Access to various web applications accessible by employees are using single-sign-on using two-factor authentication (Google Oauth) and require a Virtual Private Network (VPN) when working remotely
    c. Administrator access to Crobox Platform Management interface is only allowed by VPN
2. Production environment related:
    a. Logging in to the servers is only possible by means of public / private key exchange; passwords are not used
    b. Administration panel requires two factor authentication
    c. All security updates are automatically installed and the server is always up-to-date
    d. Strict firewall configuration from the public internet. Only allowing HTTP and HTTPS access on load balancers
    e. Communications to and from the servers, as well as backups, are only performed via secured channels (SSL / HTTPS
    f. SSH only accessible by private VPN
    g. Active monitoring (graylog + alerts) and banning of incorrect login attempts (fail2ban)
    h. All (virtual) servers are hosted externally
3. About Personal Data:
    a. All data is pseudonymised
    b. All personal data is kept using a retention period
    c. Graylog required for system monitoring has a retention period of 30 days max
    d. Backup data is stored in proprietary binary format ("*pseudo encrypted"*) and separated per client
    e. Please consult our separate 'Personal Data Document' for more detailed information, see 5.1 Downloadable content

3.2.2 Hosting & Infrastructure

Crobox hosts its complete infrastructure at Tilaa, see https://www.tilaa.com/. Tilaa is headquartered in Amsterdam, the Netherlands and is ISO 27001, ISO 9001, PCI-DSS, NEN 7510 and ISAE 3402 certified.

All of our (virtual) servers and all our data storage is located within the European Union. This includes our backup copies stored in Amazon Web Services S3 (AWS), which designated location Ireland.

3.2.3 Pseudonymisation

Personal Data is pseudonymised by design and by default. Since we don't store any unique identifiable information[1] per Data Subject other than the UUID (see 2.3.3 Unique Identifier (UUID), it is simply impossible to 'know' which natural person is behind the personal data. As a result, our database is 'useless' without being the owner of the UUID itself; there is simply no possibility to determine of retrieve the natural person behind the data.

3.2.4 Encryption

Since no contact or identifiable information is stored in our databases, we don't see a direct need to encrypt Personal Data; without encryption the data is still completely useless without being the owner of the UUID.

That said, all personal data that is stored is wrapped in a special binary format that is only known by Crobox. The contracts and specifications required to 'understand' these binary streams are safely kept and guarded within Crobox and are not exposed to the public.

3.2.5 Data Storage

All data silo's are installed & managed in our own infrastructure, except for Amazon S3, which is located in Ireland. Each data silo can only be accessed by our Virtual Private Network:

- Public network traffic is using SSL;
- Private network traffic is currently unencrypted. We use HTTPS termination on LB.

3.2.6 Data Accessibility

For auditing & development purposes we've installed business intelligence / data science tools/platforms in order to provide centralized access to all data sources and/ or silo's. Currently we only have two Enterprise Open Source technologies installed and available, e.g. Zeppeling & Superset. Both tools are only available from our own office network or by private VPN. Also, access to these data access tools are restricted to developers only and are secured using Google Authentication & Authorisation protocols - OAuth.

Our data silo's are also accessible by so called DBA (i.e. Database Administrators) using native clients which are installed on our infrastructure. These clients can only be accessed from our own VPN and using SSH (public/private) keys.

[1] E.g. Name, address, IP address, contact details, etcetera

3.2.7 Data Transformation

All our data processing is based on *events*; single small pieces of immutable data that encapsulate an unique event that occurred in the past. We use these events to construct data representations and/or data profiles, and since events are immutable direct data transformation is not possible by default.

Other than correcting data belonging to a Data Subject (see 5.2 Personal Data Governance) it is not possible to alter or correct data stored in our data silos, with the sole exclusion of Database Administrators.

3.2.8 Data Monitoring

We closely monitor data access and transformation. Audit logs of who accessed data is in place and stored for unlimited period. We currently only monitor our centralised data access interfaces; native clients are not monitored.

3.3 Organisational Measures

3.3.1 Security

We have the following organisational measures in place concerning security:

1. Centrally organised public key (key) registration for access to the servers; a key can be withdrawn within several minutes (during office hours on Monday to Friday and between 9.00 a.m. and 5:00 p.m. Dutch time)
2. Code-review is required for all software that communicates with the Database
3. Use of a development model for software that works with small updates on each occasion in order to minimise the security impact of the updates
4. Only the employees who must maintain the Database server have access
5. Audit-logging of all attempts to log in to the Database server
6. Employees cannot physically access the servers
7. All employees are obliged to maintain confidentiality (see 4.3.2. Confidentiality)
8. Backup system enabling (disaster) recovery to be carried out within several hours (during office hours on Monday to Friday and between 9.00 a.m. and 5:00 p.m. Dutch time)

3.3.2 Confidentiality

All employees of Crobox have signed an explicit clause in their employment contract that enforces confidentiality during the employment contract as well as thereafter - regardless of the manner in which and the reasons for which the employment contract has ended -, to refrain from making any statement to third parties, in any way, directly or indirectly, or in any form,

about data of a confidential nature in connection with the business of Crobox and/or businesses affiliated with it.

3.3.3 Subcontracting

Crobox does not work with any subcontractors that provide services that relate directly to the provision of the principal services as described in this document.

About ancillary and auxiliary services provided by third parties (e.g. telecom, hosting); where possible Crobox makes appropriate and legally binding contractual arrangements and take appropriate inspection measures to ensure the data protection and the data security of the Client's data, even when such services are outsourced.

3.4 Penetration Tests (Article 35)

As part of the Data Protection Impact Assessment (Article 35) Crobox is regularly subject to *penetration tests* (i.e. Pentests) executed by a Client, a (Data) Controller or a designated external and objective party capable thereof.

Pentests are primarily done at the request of the Client but also might be initialised by ourselves, especially after major changes and/or upgrades. The results of the pentests authorized by ourselves -whenever available- might be made publicly available or sent to a Client upon written request.

Pentests are part of Data Protection Impact Assessment (Article 35)

3.5 Bug Bounty Programs

Crobox is a proud member of Hacker One, which considers itself The Most Trusted Hacker-Powered Security Platform, see https://www.hackerone.com/

"HackerOne Response is a solution for organizations to receive and manage security vulnerability reports from external third parties. Designed to be compliant with responsible disclosure best-practices as recommended and mandated by industry associations and government entities, HackerOne Response reduces the risk of critical security disclosures surfacing on unauthorized channels by giving your team the visibility and tools they need to take action."

Over the last 1.5 years Crobox several trusted community members of Hacker One helped us with stabilizing and upgrading our security standards & measures to meet -and even exceed- those expected.

3.6 Quality Assurance

Crobox complies with the statutory requirements referred to in Articles 28 to 33. Accordingly, Crobox ensures compliance with the following requirements:

1. Crobox has designated a Data Protection Officer. See 8.2. Data Protection Officer for contact details.
2. Crobox ensures an appropriate level of (data) protection through 4. Technical and Organisation Measures.
3. Crobox offers Client full support with regard to prior consultation of any supervisory authority.
4. Crobox periodically -at least once a year- monitors its internal processes and the Technical and Organisational measures to ensure that its services and data processing complies to all requirements of applicable data protection law and the protection of the rights of the Data Subject
5. Client is entitled to verify quality assurance of the services provided by Crobox and offered to ensure quality control

4 Data Governance

4.1 Client Data Governance

4.1.1 Copies & Duplication

Copies and/or duplicates of Client's data shall never be created without explicit request and written approval of the Client, taken into account the following exceptions:

1. Backup copies as far as they are necessary to ensure a continuous service, and
2. Data required to meet regulatory requirements (for retaining data).

4.1.2 Termination

Not later than 4 weeks after termination of the Services between Crobox and Client, or earlier upon explicit written request by Client, Crobox shall delete any data that is collected, constructed or generated by any service provided by Crobox as described in this document.

This include:

1. All documents,
2. All collected data,
3. All backup data, and

4. All constructed data (including insights)

Documentation which is used to demonstrate orderly data processing in accordance with this Service Agreement shall be stored beyond the contract duration taken into account respective retention periods. Crobox might hand-over this documentation to Client in order to relieve its contractual obligation

In case of deletion, Crobox shall provide Client evidence by handing over a log of all deleted material. Additionally, Client might request an inspection in order to validate that all it's data is accordingly removed.

Deletion of Client Data includes all Personal Data of all Data Subjects belonging to Client. Trivially this results in no more access, correction or data portability for any Data Subject since all their data is deleted.

4.1.3 Backup Copies

All backup files are stored in a highly secured digital environment (Amazon AWS), only accessible by Crobox employees using private keys over SSL.

4.1.4 Export

Crobox offers Client data export functionality of all data collected and/or processed by Crobox. Data will be provided in raw electronic format (JSON) that is machine readable and widely considered an interoperable format / standard.

4.2 Personal Data Governance

As part of the GPDR, Data Subjects (e.g. natural persons or website visitors in our context) can manage their personal data collected and/or constructed by Crobox Services through the Client's website.

4.2.1 Consent (Article 6,7,8)

As required by GDPR, Data Subjects are required to provide explicit consent to any data processing related activities, see article 6 and 7 of GDPR.

Crobox does not store the Data Subject's consent regarding processing it's personal data. It's the obligation of the Controller and/or Client to take care of this regulation and take care of Data Subject's consent.

Keep in mind that whenever a Data Subject is less that 16 years old, additional regulations apply (Article 8)

4.2.2 Right to Rectification (Article 16)

Part of the GPDR is the right for each Data Subject to alter, adjust or correct it's Personal Data. At the current time of writing it is unclear if this right only affects information provided *directly* by the Data Subject or not.

From a compliance perspective it is rather impossible for Crobox to provide the Data Subject a means to change all constructed and aggregated information -e.g. Personal Data- that is *not directly* provided by the Data Subject; this would simply interfere and corrupt the integrity of all data, its logical processing and finally mess up reporting completely. Therefore we've decided to only focus on providing functionality to modify Personal Data directly provided by the Data Subject.

This simplifies things since Crobox does not receive nor collect any Personal Data directly from the Data Subject other than the UUID, which can't be changed since it would else break the relationship with the Data Subject. As a logical consequence hereof we don't need to comply to this right at the current moment.

4.2.3 Right to Erasure (Article 17)

By means of our available Personal Data Portal individuals can *instantly* delete and remove all their personal data. Due to obligations as set forth in the GDPR and law, backup copies are not affected. However, blacklists are carefully maintained containing all user id's that are deleted, so that whenever a (disaster) recovery takes place, information belonging to deleted profiles is not ignored and thus not restored

Crobox has taken the following -technical and organizational- measures when a Data Subject requests her data to be deleted:

1. Our primary store of record is given the nature of storing and processing big data constructed as 'write append', making it impossible to 'truly' delete data. In order to delete personal data, we ensure that:
    a. All records belonging to given Data Subject as marked as deleted, and
    b. Replace all personal data (e.g. column fields) with either zeros or blank values.
2. We add the unique user identifier to a whitelist so that when (emergency) backups are restored, all personal data belonging to 'deleted' Data Subjects is automatically removed (e.g. not inserted into the primary store of record) and/or adjusted according to above described measures when this is not technically possible,
3. When data is deleted, Crobox provides proof by handing over a log of all data deleted when available (Article 19),

4. System data (including system & activity logs) can't be deleted. However, these data is only kept for limited period (max 30 days)

Since Crobox does not store any personal contact information, it is important to understand / note that Crobox:

1. Can't accept direct requests of Data Subjects to delete data and/or to-be-forgotten based on any contact information such as email, name and/or address. In order to delete data we need the unique UUID representing the Data Subject in consideration. This UUID is stored in a Cookie (e.g. directly possessed by the Data Subject) and might be stored by Controller along with other (personal) contact details
2. Can't email or (electronically) send the log since we don't have this email. However, at the Data API

Deletion of Personal Data does **not** stop (current & future) processing of Personal Data. In other words, new personal data will be collected and new profiles will be built. To halt current and future processing please see 5.2.4 Right to Restriction of Profiling (a.k.a. Opt-out) (Article 18)

4.2.4 Right to Restriction of Profiling (a.k.a. Opt-out) (Article 18)

Using our Personal Data Portal, end consumers can opt-out. After opting out, the Crobox tracking cookie[2] if available will be deleted and a new cookie will be set indicating that specific user doesn't want to be tracked over (new) sessions.

After opting out, no (personal) data will be collected, updated or processed and/or updated any more. As a logical consequence, after opt-out an end customer will not experience any of Crobox services as set forth in this Service Agreement any more.

After opt-out, the (current & future) processing of Personal Data stops, but the Personal Data will **not** be deleted.

A clear (visual) indication will be provided in the Personal Data Portal that shows that current processing is halted (Article 19).

4.2.5 Right to Data Portability (Article 20)

By means of our available Personal Data Portal Data Subjects can at all times obtain an instant and up-to-date overview of all their personal data. Data will at minimum be presented by means of *event data* in raw electronic format (e.g. JSON), that is machine readable and widely considered an interoperable format.

[2] See 12. Appendix A: Crobox Cookie Policy

That said, we're working on a visual interface (e.g. the Personal Data Portal) that offers the Data Subject a clear overview of all personal data collected and represented in an understable way.

4.2.6 Right to Object (Article 21)

Since in our case the right to object and the right to restrict processing are the same, please see 5.2.4 Right to Restriction of Profiling (a.k.a. Opt-out) (Article 18).

4.2.7 Automated individual decision-making (Article 22)

The right not to be subject to a decision based solely on automated processing, including profiling, is for Crobox identical to the right to restrict processing, see 5.2.4 Right to Restriction of Profiling (a.k.a. Opt-out) (Article 18).

4.2.8 Backup of Personal Data

Personal data is included in Client's data and stored altogether in encrypted format and kept in a highly secured digital environment (Amazon AWS), only accessible by Crobox employees using private keys. Thus we do not create individual backup copies per Data Subject.

4.2.9 Costs inferred with Data Subject's Rights (Article 12.5)

As clearly stated in the GDPR, all services associated with the personal rights of Data Subjects, e.g. all services found in 5.2 Personal Data Governance, are provided free of charge.

That said, when requests from a Data Subject are manifestly unfounded or excessive, Crobox has the right to charge administrative costs (Article 12.5)

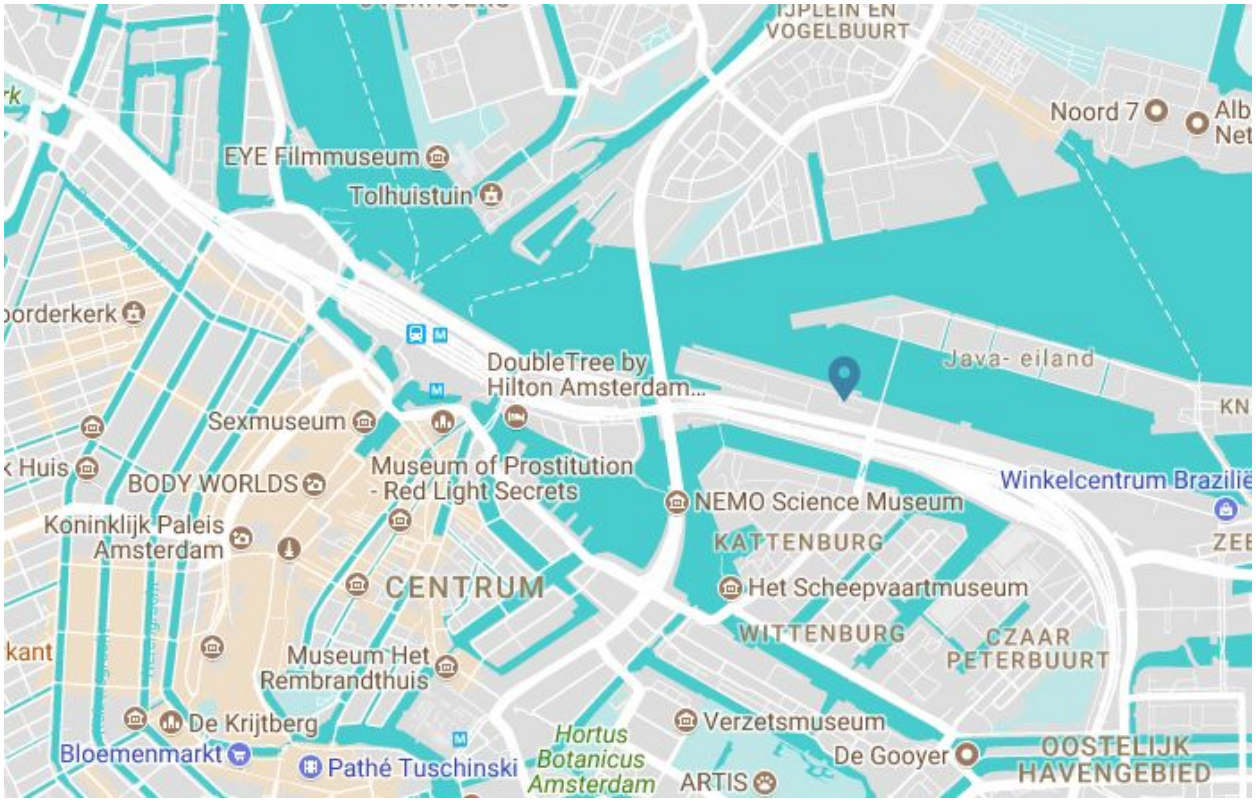
5 Contact Information

5.1 Downloadable content

The following documentation is directly available to the public and can be downloaded free of charge:

1. **General Data Protection Regulation (GDPR)**, i.e. this document. Available at: https://www.crobox.com/legal/gdpr
2. **Personal Data** - This document provides more insights about the personal data we collect. Available at: https://www.crobox.com/legal/personal_data
3. **Cookie Policy** - Available at: https://www.crobox.com/legal/cookie_policy
4. **Codes of Conduct** - Available at: https://www.crobox.com/legal/codes_conduct

5.2 Office Address



Jollemanhof 17
1019 GW Amsterdam
The Netherlands
+31 (0)88 104 4555

5.3 European Union

Crobox is headquartered in the Netherlands, which is a Member State of the European Union (EU) and a Member State of the European Economic Area (EEA).

5.4 Data Protection Officer

Crobox has a designated Data Protection Officer that complies to the provisions as set out in Article 37 of Section 4. Currently this position is hold by:

Mr. Leonard Wolters
Chief Data Officer

leonard@crobox.com
+31 (0)88 1044 555
+31 (0)6 5553 0401

5.5 Technical Security Officer

For any technical and/or security related questions, please contact:

Mr. Sjoerd Mulder
Chief Technical Officer
sjoerd@crobox.com
+31 (0)88 1044 555
+31 (0)6 5553 0401

5.6 Disclaimers

5.6.1 Compensation

Crobox might charge compensation for support services which are not included in this Service Agreement and/or are not attributable to failures on behalf of Crobox.

5.6.2 Governing Law and Jurisdiction

Services provided by Crobox including our Service Agreements are exclusively governed by the laws of the Netherlands. All disputes arising in connection with a Service Agreement, or further agreements resulting thereof, shall (in first instance) exclusively be settled by the competent court of Amsterdam, the Netherlands.

6 Appendix: Service Agreement Template

According to Article 28 of GDPR, each Data Processor is obliged to have a (Service) Agreement in place with the Data Controller. This contract needs to address some requirements that are listed below.

6.1 Subject Matter

See 2.1 Subject Matter

6.2 Duration

Unless other specified, our Services are authorised for an unlimited period and can be cancelled by either Party (that is: Crobox and/or Client) with a notice period of 3 months. This does not prejudice the right to terminate the Service Agreement without notice,

6.3 Nature and Purpose

See 2.2 Nature and Purpose

6.4 Type of Personal Data

See 2.3.4 Personal & Sensitive Data (Article 9)

6.5 Categories of Data Subjects

See 2.3.2 Categories

6.6 Explicit Instructions

Crobox requires the **explicit and written instructions** of the Client for any Data Processing, unless required to do so by Union or Member State Law. Without these instructions Crobox won't offer its Services and can't be held responsible for any claim and/or damage.

6.7 Waiver Transfer Personal Data

The undertaking of the contractually agreed Processing of Data (Service Agreement) shall be carried out exclusively within a Member State of the European Union (EU) or within a Member State of the European Economic Area (EEA).

Each and every transfer of data to a state which is not a Member State of either the EU or the EEA requires the prior agreement of the Client and shall only occur if the specific Conditions of Article 44 et seq. GDPR have been fulfilled.

The adequate level of protection in …….. (e.g. country, territory or specific sectors within a country)

- has been decided by the European Commission (Article 45 Paragraph 3 GDPR),
- is the result of binding corporate rules (Article 46 Paragraph 2 Point b in conjunction with Article 47 GDPR),
- is the result of Standard Data Protection Clauses (Article 46 Paragraph 2 Points c and d GDPR),
- is the result of approved Codes of Conduct (Article 46 Paragraph 2 Point e in conjunction with Article 40 GDPR),
- is the result of an approved Certification Mechanism. (Article 46 Paragraph 2 Point f in conjunction with Article 42 GDPR),
- is established by other means:……. (Article 46 Paragraph 2 Point a, Paragraph 3 Points a and b GDPR)