BINDING CORPORATE PRIVACY RULES (BCPR)

Document Classification:	**Public**
Document Ref:	**BCPR-DOC-08/05**
Version:	**1**
Dated:	**8 May 2018**
Document Author:	**Rob de Haas**
Document Owner:	**Rob de Haas**

REVISION HISTORY

Version	Date	Revision Author	Summary of Changes
V2	31 May 2019	Speed Jiang	Updates to doc/link references

Distribution

Name	Title

Approval

Name	Position	Signature	Date

Contents

1 INTRODUCTION TO SEEDLINK'S BCPR 5
1.1 BACKGROUND & ACTIONS 6
1.1.1 What is Privacy Law and the GDPR 6
1.1.2 How does the GDPR affect Seedlink internationally? 6
1.1.3 What is Seedlink doing about it? 6
1.1.4 Information Security Manager 7
1.1.5 Third-party beneficiary clause 7
1.1.6 How does Seedlink process data? 8
1.1.7 People Insights Flow-chart 8
1.1.8 Client cloud environment Requirements 8
2 THE BINDING CORPORATE PRIVACY RULES (BCPR) 9
2.1 : COLLECTING AND USING PERSONAL IDENTIFIABLE INFORMATION 10
2.2 PRACTICAL COMMITMENTS MADE BY SEEDLINK 12
3 PERSONAL IDENTIFIABLE INFORMATION REQUEST PROCEDURE² 13
3.1.1 Approach 13
3.1.2 Seedlink response 14
3.1.3 What happens if an individual, disputes a response? 15
4 INCIDENT RESPONSE PROCEDURE IN CASE OF A BREACH 16
4.1.1 Incident Detection and Analysis 16
4.1.2 Activating the Incident Response Procedure 16
4.1.3 Assemble Incident Response Team 17
4.1.4 Seedlink response 17
4.1.5 Incident Response Flowchart 20
5 AUDIT PROTOCOL 21
5.1.1 Monitoring and Measurement 21
5.1.2 Analysis and Evaluation 21
5.1.3 Approach 22
5.1.4 Resources 22
5.1.5 Schedule 22
5.1.6 Communication of Findings 22
5.1.7 Providing Audit Reports to European Data Protection Authorities 22
5.1.8 Audits by European Data Protection Authorities 22
5.1.9 Co-operation Procedure between Seedlink companies 23
5.1.10 Co-operation with European Data Protection Authorities 23
6 UPDATE PROCEDURE 24

6.1.1 Approach 24
6.1.2 Communicating changes to Seedlink SCL and Individuals 24
6.1.3 Inclusion of new Seedlink locations 24
7 APPENDIX I IRT Team and Roles 25
8 APPENDIX II Acronyms 27

1 INTRODUCTION TO SEEDLINK'S BCPR

These Binding Corporate Privacy Rules ('**BCPR'**) establish Seedlink's approach to compliance with privacy law, also known as data protection law and/or the General Data Protection Regulation (EU) 2016/679 ('**GDPR**'), and specifically to transfers of personal data between Seedlink's corporate locations. Seedlink's corporate locations ('**SCL**'[1]) and their employees must comply with and respect the BCPR when collecting and using personal data. Additional privacy compliance requirements may apply to specific business areas or functions. The BCPR apply to all personal data related to employees, customers, suppliers, candidates and other individuals, collected and used by Seedlink. The BCPR also apply where SCL process personal data on behalf of their customers and other SCL. The BCPR are communicated to all of Seedlink's employees and published on the external Seedlink website accessible at https://cdn-eu-aws.slaimg.com/policies/seedlink-binding-corporate-privacy-rules-20190611.pdf.

_____

[1]HQ in Amsterdam, Netherlands, will act as EU Main Establishment[2]. Other SCL include Seedlink's Shanghai Office.

[2]A Main Establishment is the authority with the primary responsibility for dealing with a cross-border data processing activity.

FURTHER INFORMATION

If you have any questions about the Binding Corporate Privacy Rules (BCPR), your rights under these BCPR or any other privacy issues you can contact the Seedlink Privacy & Security team at the address below.

Email: security@seedlinktech.com

Or offline;

EU Main Establishment
Seedlink Technologies BV
Kleine Gartmanplantsoen 21 (2nd Floor)
1017 RP Amsterdam
The Netherlands

1.1 BACKGROUND & ACTIONS

1.1.1 What is Privacy Law and the GDPR

Privacy law, also known as "data protection law" in some countries, gives individuals the right to control how their "personally identifiable information[1]" (PII) is used and sets out how organizations must manage and protect that information. In addition, the GDPR replaces the Data Protection Directive 95/46/EC and was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens data privacy and to reshape the way organizations across the region approach data privacy.

[1]Personally identifiable information (PII) is any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered PII.

1.1.2 How does the GDPR affect Seedlink internationally?

The GDPR applies to the processing of personal data or PII, by controllers and processors in the EU, whether the processing takes place in the EU or not. The GDPR also applies to the processing of personal data of data subjects in the EU by a controller or processor not established in the EU, where the activities relate to: offering goods or services to EU citizens (irrespective of whether payment is required) and the monitoring of behavior that takes place within the EU. Non-EU businesses processing the data of EU citizens must appoint a representative in the EU.

SCL[1] transfer personal identifiable information to other SCL for a variety of reasons connected to the technical and operational requirements of the business. For example, personally identifiable information about employees may be transferred for the administration of employee payroll and benefits or for Seedlink's internal employee education and development programs. Another example is the transfer of customer personally identifiable information to provide products or technical support services.

- Entity 1: EU HQ Seedlink Technologies BV Main Establishment Netherlands, Amsterdam – data processor
- Entity 2: CN Seedlink Technologies China, Shanghai – data processor

[1]When Seedlink transfers personally identifiable information between countries, Seedlink provides an adequate level of protection for that information in compliance with the GDPR

1.1.3 What is Seedlink doing about it?

Respecting privacy is fundamental to Seedlink's culture and helps us maintain an environment where individuals can trust Seedlink and our technology. The BCPR are designed to provide an adequate level of protection for all personal data collected and used by Seedlink. The BCPR apply in all cases where Seedlink collects and uses personally identifiable information, whether online or offline, or by manual or automatic means. The BCPR apply worldwide and ensure that Seedlink's collection and use of personal data complies with the GDPR. Most transfers of personally identifiable information take place between Seedlink's companies worldwide and personally identifiable information may flow between any SCL.

1.1.4 Information Security Manager

Seedlink's Information Security Manager (ISM) is responsible for overseeing and ensuring compliance with the BCPR for all SCL within and outside of Europe, supported by EU HQ Seedlink Technologies BV Main Establishment Netherlands ('**EU LSA**'), and a matrixed network of Seedlink Technical Staff, responsible for enabling compliance with the BCPR on a day-to-day basis. The ISM's responsibilities include advising Seedlink's management as required, working with national data protection authorities, *Autoriteit Persoonsgegevens* (the Dutch privacy authority) and oversight of the Seedlink EU Main Establishment in Amsterdam.

Seedlink's ISM is responsible for ensuring that changes to the BCPR are notified to all SCL and to individuals whose personal data is processed by Seedlink. If an individual, whose information is collected and/or used by Seedlink, believes Seedlink has not complied with the BCPR, that individual may raise the matter with Seedlink's ISM.

Individuals whose personal data is collected and/or used by a SCL in Europe and transferred to SCL outside Europe may exercise certain rights before the competent courts and/or national data protection authorities, such as the Dutch privacy authority, *Autoriteit Persoonsgegevens ('***AP***').*

These rights are outlined in Seedlink's Terms & Conditions (T&C) https://cdn-eu-aws.slaimg.com/policies/seedlink-technologies-terms-and-conditions.pdf?v3.1 and Seedlink's Privacy Policy (SPP) https://cdn-eu-aws.slaimg.com/policies/seedlink-technologies-privacy-policy-20190611.pdf.

If an individual can demonstrate they have suffered damages and can establish facts which show the damage has likely occurred because of a breach of the BCPR, the SCL in Europe accepts the burden of proof to show that Seedlink's entity outside Europe was not responsible for the breach of the BCPR or that no breach took place. If the SCL can prove that the SCL outside of Europe is not responsible for the event that led to the damages, the SCL can discharge itself from any responsibility.

The T&C and SPP bind SCL to comply with the BCPR if personal data is collected, used and transferred from (one of) SCL based in Europe to (one of) SCL established elsewhere.

1.1.5 Third-party beneficiary clause

Some of the rights set out in the T&C and SPP are summarized hereafter and may be invoked by third parties to:

1. externally enforce Seedlink's compliance with the BCPR, including its appendices;
2. lodge a complaint before a European data protection authority of competent jurisdiction and/or before the courts of the jurisdiction in which the particular Seedlink company that is responsible for exporting such personal data is established or the courts in the Netherlands, in accordance with the laws of the Netherlands, and also to enforce compliance with the BCPR;
3. make complaints to a Seedlink company within Europe, seek appropriate redress from the national privacy authority such as the AP, including the remedy of any breach of the BCPR by any Seedlink company outside Europe and, where appropriate, receive compensation from Seedlink for any damage suffered because of a breach of the BCPR in accordance with the determination of a court or other competent authority; and/or
4. make complaints to a Seedlink company outside of Europe in case of a breach of the BCPR with that Seedlink company as far as it concerns personal data that is transferred out of the EU within the Seedlink Group (this article does not apply to other personal data). Seedlink's

companies outside of the EU are bound by the BCPR as well. A complaint about a possible breach of the BCPR can be addressed according clause 3.1.1., but if the complaint is not handled in compliance with the BCPR, Seedlink's EU LSA HQ accepts liability for such breaches. This liability only extends to data transferred from the EU under the rules.

5. Third parties are able to enforce principles such as; purpose limitation; data quality and proportionality; criteria for legitimate processing; transparency and easy access; right of rectification, erasure, blocking of data and objecting to the processing; rights in case automated individual decisions are taken; security and confidentiality; restrictions on onward transfers outside the Seedlink group; national legislation preventing the respect of the BCPR; right to complain Seedlink's internal complaint mechanism; cooperation duties with DPA; liability and jurisdiction provisions; and their rights relating to automated decision making and profiling.
6. the SCL who is charged with a breach, in whole or in part, shall be exempt from that liability only if it proves that it is not responsible for the event that led to damages
7. obtain a copy of the BCPR, T&C and SPP on request.

1.1.6 How does Seedlink process data?

The only way Seedlink processes data is through its service People Insights. An A.I. based machine learning solution processes employee and candidate data such as name, email address, cv and the candidate and/or employee's answers to open & closed ended questions. The data processed flows between the candidates/employees of a certain client of Seedlink and that client, through People Insights. Seedlink's clients are mainly companies who use Seedlink's People Insights for recruitment, training and/or internal mobility purposes. Seedlink's clients generally qualify as controllers when it comes to processing personal data and have their own responsibilities to comply with the GDPR when it comes to controlling and processing the personal data of their candidates/employees.

1.1.7 People Insights Flow-chart

The Seedlink EU LSA is using the datacenter of Amazon Web Services (AWS) as the main infrastructure for Europe for storage and archiving, and assigned a datacenter in Germany, as back-up. Seedlink China uses Aliyun servers in Hangzhou. Client modules are built in Europe and make use of the datacentre of Amazon Web Services. Currently Seedlink is using the access portals described below;

- Chinese clients use https://cn.app.seedlinktech.com/
- European & other non-Chinese clients use https://eu.app.seedlinktech.com/

1.1.8 Client cloud environment Requirements

1. People Insights HR accounts must always be protected by a username and a password. To gain access an extra validation is required through a One Time Password (OTP) request. The OTP will be sent either to the persons email or can be generated through an authenticator application running on their mobile phone.
2. The People Insights model offers Role based protection. Different persons of the company can access or view the candidate's data and have their personal username and password. Rights are given by the Engagement Manager at first and maintained by the HR-project leader during the project. All HR-users use the validation protection through OTP by default

3. Seedlink's Engagement Manager is responsible for distributing access to the platform on role-based principles. Requesting access for a new person from a certain client must be filed with the responsible Seedlink Engagement Manager who will decide whether access is granted and what security levels and options are associated with the access granted
4. Seedlink's clients that qualify as data controllers have their own responsibilities and obligations to protect personal data of (for example) their employees and candidates. Seedlink's Engagement Manager complies with Seedlink's BCPR.
5. It is the responsibility of Seedlink's Engagement Manager to inform the client, as a data controller, about Seedlink's BCPR relating to the EU GDPR regulation 2016/679
6. It is the responsibility of Seedlink to provide accurate information & services and opportunities to ask questions and file complaints for candidates, employees, and the client.
7. Seedlink can use data for science & research purposes and is obligated to notify the candidates and clients through Seedlink's T&C and SPP regulation
8. Candidates and employees should always be informed of their rights which include, the right of access, the right to rectification, the right to erasure/be forgotten, the right to restrict processing, the right to data portability, the right to object, and their rights relating to automated decision making and profiling.

2 THE BINDING CORPORATE PRIVACY RULES (BCPR)

2.1: The BCPR that Seedlink must observe when collecting and using personal identifiable information.

2.2: The practical commitments made by Seedlink to the European data protection authorities.

2.1 : COLLECTING AND USING PERSONAL IDENTIFIABLE INFORMATION

RULE 1 – COMPLYING WITH NATIONAL LAWS: Seedlink will ensure personal identifiable information is collected and used in compliance with national laws.

Where the BCPR or company guidelines differ from national laws or regulations, Seedlink will always comply with the higher standard. The BCPR also apply if (one of) SCL process(es) personal data on behalf of another SCL.

RULE 2 – ENSURING TRANSPARENCY, FAIRNESS AND LAWFULLNESS: Seedlink will honor those principles and explain to individuals how their personal data will be used by Seedlink.

Seedlink will provide clear and comprehensive notice when personal data is collected describing how the personal data will be used and who it will be shared with, unless there is a legitimate basis for not doing so.

RULE 3 – USING PERSONAL IDENTIFIABLE INFORMATION FOR A VALID PURPOSE: Seedlink will only collect and use personal identifiable information for purposes which are relevant to Seedlink, research and science, and are known to the individual or which are within their expectations.

If Seedlink changes the purpose for which personal identifiable information is used, Seedlink will make individuals aware of the changes, unless the changes are within the individual's expectations and they can express their concerns, or unless there is a legitimate basis for not doing so. If Seedlink changes the purpose for which personal identifiable information is used, Seedlink may be required to ask the individual(s) concerned for their consent.

RULE 4 – ENSURING DATA QUALITY: Seedlink will only collect and use personal identifiable information that is relevant and not excessive for the purpose.

Seedlink will keep personal identifiable information accurate and up to date. Seedlink will only retain personal data for as long as that is necessary to achieve the lawful purpose the data was collected for or to comply with other legal requirements (see Rule 3). Seedlink provides individuals with a choice of methods to access and amend personal identifiable information and communication preferences, including online, in writing (including email), or by contacting the appropriate Seedlink contact centers or offices.

RULE 5 – TAKING APPROPRIATE SECURITY MEASURES: Seedlink will implement appropriate technical and organizational measures to protect personal identifiable information.

Seedlink applies technical and organizational measures appropriate to the risks presented by the processing of personal data. If (on) SCL process(es) personal data on behalf of another SCL, all SCL will adhere to the BCPR and act only in accordance with the instructions of the SCL on whose behalf the processing is carried out.

RULE 6 – HONOURING INDIVIDUALS' RIGHTS: Seedlink will respond to inquiries or requests made by individuals about their personal identifiable information.

1. Seedlink will reply to requests to rectify, delete, block or cease processing personal data.
2. Seedlink will respond to requests from individuals whose personal data is collected and used by Seedlink, in accordance with the Personal identifiable information Request Procedure (see Chapter 3).

RULE 7 – PROTECTING PERSONAL IDENTIFIABLE INFORMATION TRANSFERRED TO THIRD PARTIES: Seedlink will ensure that personal identifiable information transferred to third parties is adequately protected.

Transfers of personal data to third parties outside Seedlink are not allowed without appropriate steps being taken to ensure that there is a legal basis for the transfer and to protect and secure the personal data being transferred, such as contractual clauses, whether the third party is a data controller or a service provider. For example, where a third-party service provider processes personal data on behalf of Seedlink, Seedlink will enter into a contract with that provider which states that the third-party service provider will act only on Seedlink's instructions and will adopt proportionate technical and organizational security measures to safeguard the personal data. Appropriate technical and organizational measures to protect personal identifiable information are also applied during the transfer of the personal data to a third party. Validation of security measures implemented by third-parties takes place during the procurement process and is repeated periodically as required, for example in response to contract renewal or changes in business, legal or regulatory requirements.

RULE 8 – SAFEGUARDING THE USE OF SENSITIVE PERSONAL IDENTIFIABLE INFORMATION: Seedlink will only use sensitive personal data if it is necessary and where the individual's express consent has been obtained, unless Seedlink has an alternative legitimate basis for using the information.

Sensitive personal identifiable information is information about an individual's racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, health, sex life and criminal convictions, in other words, personal data that could be identified to the person itself directly or indirectly. Seedlink will assess whether the collection and use of sensitive personal identifiable information is required for the proposed use and when it is necessary in the context of the business. Individuals must expressly agree to the collection and use of their sensitive personal identifiable information by Seedlink, unless there is an alternative legitimate basis for collecting and using the information. Seedlink classifies personal data based upon its level of sensitivity. Seedlink implements appropriate technical and organizational measures to protect sensitive personal identifiable information, based on that classification (also see Rule 5).

RULE 9 – USING PERSONAL IDENTIFIABLE INFORMATION FOR DIRECT MARKETING: Seedlink will not use personal identifiable information for direct marketing to a consumer unless the consumer has agreed to that use.

Seedlink will give all individuals the opportunity to opt out of receiving direct marketing from Seedlink. Seedlink will honor the opt out requests it receives. Seedlink will identify and clearly explain the purposes for which personal identifiable information will be used as described in Rule 2. Individuals have the right to object to the collection and use of their personal identifiable information for direct marketing purposes. Seedlink will provide individuals with a choice of methods to access and amend personal identifiable information and communication preferences for direct marketing (see Rule 4).

RULE 10 – MAKING AUTOMATED DECISIONS: Seedlink will explain the logic used to make an automated decision about an individual, upon request.

Individuals that are subject to a decision based only on automated processing of personal identifiable information are entitled, by making a written request to Seedlink, to know the logic involved in the decision. [*SECTION B – PRACTICAL COMMITMENTS MADE BY SEEDLINK*]

2.2 PRACTICAL COMMITMENTS MADE BY SEEDLINK

RULE 11 – TRAINING: Seedlink will provide appropriate training to employees who collect, use or access personal identifiable information, or who are involved in the development of products, services or tools used to process personal identifiable information.

RULE 12 – AUDITING: Seedlink will follow the Audit Protocol set out in Chapter 4.

RULE 13 – HANDLING COMPLAINTS: Seedlink will follow the Complaint Handling Procedure set out in Chapter 3.

RULE 14 – CO-OPERATING WITH DATA PROTECTION AUTHORITIES: Seedlink will follow the Co-operation Procedure set out in Chapter 4.1.9.

RULE 15 – UPDATING THE BCPR: Seedlink will follow the Update Procedure set out in Chapter 5.

RULE 16 – CONFLICTING LEGAL REQUIREMENTS: If Seedlink becomes aware of a conflict between national law and the BCPR which would prevent Seedlink from complying with the BCPR, Seedlink's ISM will be promptly informed of such a conflict. The ISM will decide how to resolve the issue and will consult with the appropriate data protection authority if necessary.

3 PERSONAL IDENTIFIABLE INFORMATION REQUEST PROCEDURE[2]

Seedlink has an Information Security Management System[1] (ISMS) in place which conforms to the ISO/IEC 27001 international standard. The ISMS helps to provide governance and control of the framework Seedlink uses to protect its information assets and reduce its risk. It is important that everyone involved in the ISMS understands their role and how the activities they perform contribute to meeting business and information security requirements and the overall objectives of Seedlink's organization.

_____

[1]A full description of the interested parties of the ISMS is set out in the document Information Security Context, Requirements and Scope and this is summarized here.
[2]This chapter is based on the document ISO27001 *ISDM-DOC-A16-2 Information Security Incident Response Procedure*

The purpose of the Seedlink Binding Corporate Privacy Rules (BCPR) is to establish Seedlink's approach to compliance with the GDPR. An individual can make a request to obtain personal identifiable information collected ('**Request**'). If that personal identifiable information is shown to be inaccurate, the individual may ask for that information to be corrected, deleted or blocked and, in certain circumstances may object to the processing of their personal identifiable information. Seedlink will consider such requests and deal with them as appropriate.

3.1.1 Approach

The general approach to ensuring effective engagement and communication with respect to the ISMS within Seedlink is as follows:

1. Identify the audience/interested parties
2. Define the appropriate communication topics for each interested party
3. Agree on the most appropriate methods of engagement and communication
4. Implement the program
5. Obtain and act on feedback about the success of the communication, via input to the continual improvement plan

Seedlink will respond to individuals who make a Request without undue delay and in any event within one month of receipt of the request. That period may be extended by a maximum of two months, in which case Seedlink will inform the data subject accordingly. This includes Requests that are not presented in a formal manner, or that may not specifically mention privacy or data protection law. Personal data covered by a Request may include the personal data about the individual Seedlink collects and uses, including a description of the personal data, the purposes for which the information is used, and a description of transfers of that personal identifiable information to others.

An individual wishing to make a Request can do so:

Online: https://seedlinktech.zendesk.com/hc/en-us/requests/new

Email: security@seedlinktech.com

or

Offline in writing:

EU Main Establishment
Seedlink Technologies BV
Kleine Gartmanplantsoen 21
1017 RP Amsterdam
The Netherlands

- In addition, Seedlink's locations, programs, contact centers and employees are required to direct privacy-related enquiries to Seedlink's ISM in a timely manner.
- Individuals making a Request are required to confirm that any information they provide while making the Request is correct to the best of their knowledge and belief, and to confirm they are requesting their own personal identifiable information.

There are several other established communication methods in place within Seedlink and these will be used where possible. These include:

- Website https://www.seedlinktech.com
- Seedlink customer service system: https://seedlinktech.zendesk.com
- Email: security@seedlinktech.com
- LinkedIn company page: https://www.linkedin.com/company/seedlnk/
- Through the direct account manager
- Written: Seedlink Technologies BV, Kleine Gartmanplantsoen 21, 1017 RP Amsterdam

3.1.2 Seedlink response

- Seedlink will use reasonable endeavours to acknowledge receipt of a Request within 5 working days of the Request being received by Seedlink's Support or Security Teams.
- Seedlink will explain to individuals making Requests that it may be necessary to confirm their identity and require more detailed information to locate the requested personal identifiable information.
- Seedlink will also explain that attempting to obtain personal data to which they are not entitled may be a violation of the law. If the Request is unclear, imprecise or unreasonable, Seedlink will ask the individual to clarify what sort of personal data they are requesting and where they expect this information to be found.
- Seedlink will notify the individual of the outcome of their request within 30 days if the request is clearly understood by Seedlink. If the Request is too complex to allow a notification within 30 calendar days, Seedlink will provide the individual with an estimate of when a notification will be provided.

Unless prohibited under applicable law, Seedlink may withhold certain information, including (but not limited to) information:

- obtained or retained about the prevention or detection of crime, or that Seedlink is required to withhold in response to national or international legal requirements (for example for national security purposes);
- where necessary for legitimate business purposes;
- covered by legal professional privilege;
- relating to third parties (unless their consent has been obtained or it is reasonable to supply the data without their consent);

- relating to the protection of the individual making the request or the rights and freedoms of others;
- where the search for that data would require disproportionate effort, or have a disproportionate effect, for example due to the cost of providing the data, the time it would take to retrieve the data or how difficult it may be to obtain the data requested.
- A Request will be considered closed on the date the individual making the Request is provided with the information or is informed that Seedlink has decided not to provide the information.

3.1.3 What happens if an individual, disputes a response?

If an individual disputes Seedlink's response the individual may notify Seedlink that they do not agree with Seedlink's response and/or raise the matter with the relevant national privacy authority, such as the AP.

If the individual notifies Seedlink that he or she does not agree with Seedlink's response, the matter will be handled in accordance with section *Approach* of the Complaint Handling Procedure.

In the event of disagreement or uncertainty about if to activate an incident response, the decision of the Team Leader will be final.

In case it is decided not to activate the procedure, a plan should be created to allow for a lower level response to the incident within normal management channels. This may involve the invocation of relevant procedures at a local level.

4 INCIDENT RESPONSE PROCEDURE IN CASE OF A BREACH

Seedlink has an Information Security Management System[1] (ISMS) in place which conforms to the ISO/IEC 27001 international standard. The ISMS helps to provide governance and control of the framework Seedlink uses to protect its information assets and reduce its risk. It is important that everyone involved in the ISMS understands their role and how the activities they perform contribute to meeting business and information security requirements and the overall objectives of Seedlink's organization.

_____

[1]A full description of the interested parties of the ISMS is set out in the document Information Security Context, Requirements and Scope and this is summarized here.
[2]This chapter is based on the document ISO27001 *ISDM-DOC-A16-2 Information Security Incident Response Procedure*

The purpose of the Seedlink Binding Corporate Privacy Rules (BCPR) is to establish Seedlink's approach to compliance with the GDPR in case of a data breach.

4.1.1 Incident Detection and Analysis

The impact assessment should estimate:

- The extent of the impact on IT infrastructure including computers, networks, equipment and accommodation
- The information assets that may be at risk or have been compromised
- The likely duration of the incident i.e. when it may have begun
- The business units affected and the extent of the impact on them
- Initial indications of the likely cause of the incident

Any member of the management team has the authority to contact the Incident Response Team Leader at any time to ask him/her to assess whether the Incident Response Procedure should be activated.

4.1.2 Activating the Incident Response Procedure

Guidelines for whether a formal incident response should be initiated for any incident of which the Team Leader has been notified are if any of the following apply:

- There is significant actual or potential loss of classified information
- There is significant actual or potential disruption to business operations
- There is significant risk to business reputation
- Any other situation which may have a significant impact on the organization
- If it is decided not to activate the procedure then a plan should be created to allow for a lower level response to the incident within normal management channels. This may involve the invocation of relevant procedures at a local level.
- If the incident warrants the activation of the IR procedure the Team Leader will start to assemble the IRT.

4.1.3 Assemble Incident Response Team

Once the decision has been made to activate the incident response procedure, the Team Leader (or deputy) will ensure that all role holders (or their deputies if main role holders are un-contactable) are contacted, made aware of the nature of the incident and asked to assemble at an appropriate location.

The exception is the Incident Liaison who will be asked to attend the location of the incident (if different) to start to gather information for the incident assessment that the IRT will conduct so that an appropriate response can be determined. For detailed information about the roles involved see see *Appendix I for IRT teams, roles.*

Once an appropriate response to the incident has been identified, the IRT needs to be able to manage the overall response, monitor the status of the incident and ensure effective communication is taking place at all levels.

4.1.4 Seedlink response

This section sets out in what way Seedlink will communicate with interested parties both within and outside of Seedlink about information security. It identifies who the interested parties are and how an effective communication channel will be established.

The communication program is aimed at interested parties, both internal and external, contract and permanent, who have a part to play in the operation and development of the ISMS within Seedlink.

The interested parties include:

- Shareholders
- Board of Directors
- Suppliers
- Customers
- Regulatory bodies
- Employees of the organization
- Contractors providing services to the organization
- National or local government organizations
- Emergency services
- Trade associations, unions and industry bodies
- Public
- Investors

The communication program is intended to communicate the key items of information in the following main areas:

- The business environment in which the ISMS operates, including significant changes as and when they occur
- The overall framework of the ISMS including the vision, policies, plans and objectives that are to be achieved
- How the information security measures in place relate to the needs of the business, both now and going forward
- How the ISMS are intended to capture and fulfil the business requirements for information security
- The statutory, regulatory and contractual requirements and constraints within which the ISMS must operate
- Updates on how plans are progressing towards meeting the defined objectives of the ISMS
- Awareness of information security issues and risks and our approach to addressing them
- The level of detail required in the above areas will vary across the interested parties involved.

It is vital that effective communication is maintained between all parties involved in the incident response.

The primary means of communication during an incident will initially be face to face or by telephone, both landline and mobile. Email should not be used unless permission to do so has been given by the Incident Response Team ('**IRT**').

The following guidelines should be followed in all communications:

- Be calm and avoid lengthy conversation
- Advise internal team members of the need to refer information requests to the IRT
- If the call is answered by someone other than the contact:
  - Ask if the contact is available elsewhere
  - If they cannot be contacted leave a message to contact you on a given number
  - Do not provide details of the Incident
- Always document call time details, responses and actions
- All communications should be clearly and accurately recorded as records may be needed as part of a possible legal action later

There are several established communication methods in place within Seedlink and these will be used where possible. These include:

- Website https://www.seedlinktech.com
- Seedlink customer server system: https://seedlinktech.zendesk.com
- Email: security@seedlinktech.com
- LinkedIn company page: https://www.linkedin.com/company/seedlnk/
- Through the direct account-manager {name}@seedlinktech.com
- Written letter from: Seedlink Technologies BV, Kleine Gartmanplantsoen 21, 1017 RP Amsterdam

There may be many external parties who, whilst not directly involved in the incident, may be affected by it and need to be alerted to this fact.

These may include:

- Customers
- Suppliers
- Shareholders
- Regulatory bodies

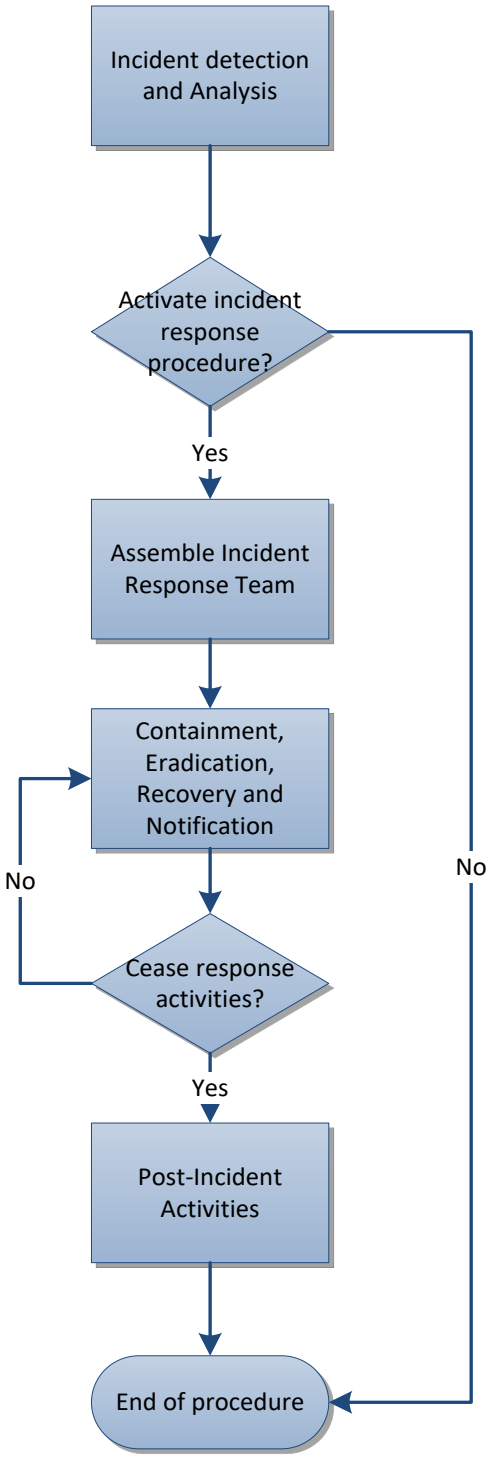
The Communications member of the IRT should make a list of such interested parties and define the message that is to be given to them. Interested parties who have not been alerted by the IRT may call to obtain information about the incident and its effects. These calls should be recorded in a message log and passed to the Communications member of the IRT.

Unless prohibited under applicable law, Seedlink may withhold certain information, including (but not limited to) information:

- obtained or retained about the prevention or detection of crime, or that Seedlink is required to withhold in response to national or international legal requirements (for example for national security purposes);
- where necessary for legitimate business purposes;
- covered by legal professional privilege;
- relating to third parties (unless their consent has been obtained or it is reasonable to supply the data without their consent);
- relating to the protection of the individual making the request or the rights and freedoms of others;
- where the search for that data would require disproportionate effort, or have a disproportionate effect, for example due to the cost of providing the data, the time it would take to retrieve the data or how difficult it may be to obtain the data requested.
- A Request will be considered closed on the date the individual making the Request is provided with the information or is informed that Seedlink has decided not to provide the information.

4.1.5 Incident Response Flowchart

The flow of the incident response procedure is shown in the diagram below.



5 AUDIT PROTOCOL

Seedlink's EU LSA (Main Establishment) provides guidance about the collection and use of personal identifiable information subject to the BCPR and assesses personal data collection and use for potential privacy-related risks. The collection and use of personal data with the potential for significant privacy impacts are therefore subject to detailed oversight and evaluation, not just during the audit process but on an on-going basis.

The international standard for information security ISO/IEC 27001:2013 (and its subsequent revisions), will be used as the basis of the criteria for the audit programme, with additional input from related standards such as ISO/IEC 27002 (information security code of practice), ISO 22301 (business continuity) and ISO/IEC 20000 (IT service management) where appropriate.

Where a discrepancy against the standard is found, one of the three types of items described below will be raised as follows:

- Observation – a comment which may be of use to the auditee, based on the experience of other ISMS implementations
- Minor non-conformity – a single lapse which does not in itself indicate a breakdown of the management system
- Major non-conformity – a significant issue which represents a breakdown of the operation of the management system

5.1.1 Monitoring and Measurement

There are many potential ways in which Seedlink can attempt to measure whether we are maintaining a good governance regime and are implementing our controls in a way that genuinely reduces risk. Some of these ways are easy to do and some are much harder; some are straightforward to interpret, and others require a lot more effort to understand what the figures may mean.

The challenge is to define a monitoring and measurement regime that gives us the answers we want without creating too much of an administrative overhead in collecting and interpreting the data.

To do this, Seedlink needs to define:

- what will be monitored and measured
- when and how the monitoring and measurement will be carried out
- when and how the results will be analysed and evaluated
- who will do each of the above
- what evidence we will keep from the monitoring and measurement results

5.1.2 Analysis and Evaluation

The main method of presentation of performance information regarding the ISMS will be a regular report. This will contain the summarised data from the measurements and will present the information graphically where possible. The ISM is responsible for the preparation of the performance reports.

5.1.3 Approach

- Seedlink will perform regular audits of compliance to the BCPR. Seedlink will ensure such audits address all aspects of the BCPR, including Seedlink's information technology systems and databases, security policies, contractual provisions, training, privacy policies and guidelines.
- Seedlink will ensure that any issues or instances of non-compliance with the BCPR identified by audits are brought to the attention of Seedlink's ISM and Seedlink's company management, and that appropriate corrective actions are taken to ensure compliance.

5.1.4 Resources

The Seedlink internal audit team will carry out the audit programme with input from the information security function and business management and staff. The resourcing of the internal auditor is reviewed on a regular basis as part of management reviews and is maintained at a sufficient level to meet its commitments.

5.1.5 Schedule

An initial audit will take place in 06/2018, which will cover all aspects of the management system. Thereafter, audits will take place every 12 months. Selected processes shall be reviewed with the intention that all processes will be covered in a 1-year timeframe. The detailed programme of audits will be maintained by the internal auditor and made available on request.

5.1.6 Communication of Findings

A draft audit report will be produced, and the contents will be communicated initially to the management team who will be given an opportunity to comment.

A plan of action to address any non-conformities and appropriate corrective actions will be agreed.

A final written report will be produced and communicated to the management team and made available to the executive team as appropriate.

Follow up visits shall take place in accordance with the plan of action to ensure any major non-conformities and corrective actions have been addressed/implemented. Such repeat visits will not be required for observations and minor non-conformities (see the introduction of Chapter 4).

5.1.7 Providing Audit Reports to European Data Protection Authorities

Seedlink will provide copies of the results of any audit of the BCPR to a European data protection authority of competent jurisdiction upon request, subject to applicable law. The data protection authority should respect the confidentiality of the information provided and any trade secrets contained in the information. Seedlink's ISM will be responsible for liaising with the European data protection authorities for this purpose.

5.1.8 Audits by European Data Protection Authorities

Seedlink's companies will co-operate and assist each other and the Seedlink EU LSA when hosting audits by national data protection authorities. This is an obligation for all SCL bound by the BCPR. Where required, Seedlink will make the necessary personnel available for a dialogue with a European data protection authority in relation to the audit reviewing compliance with the BCPR. Where appropriate, the relevant data protection authority will provide Seedlink with reasonable prior written notice of its intention to carry out an audit. Audits will be conducted during normal business hours, with full respect to the confidentiality of the information obtained and to the trade

secrets of Seedlink. Seedlink's ISM will also be responsible for liaising with the European data protection authorities for this purpose.

5.1.9 Co-operation Procedure between Seedlink companies

Seedlink's SCL will co-operate and assist each other and the Seedlink EU LSA when handling requests or complaints regarding the BCPR from individuals or national data protection authorities. Seedlink's SCL will comply with any instructions from the relevant national privacy authority, such as the AP, requiring the remedy of a breach of the BCPR

5.1.10 Co-operation with European Data Protection Authorities

Where required, Seedlink will make the necessary personnel available for dialogue with a European data protection authority in relation to the BCPR.

Seedlink will actively review and consider:

- any decisions made by relevant European data protection authorities on any data protection law issues that may affect the BCPR; and
- the views of the Article 29 Data Protection Working Party as outlined in its published guidance on Binding Corporate BCPR.

Seedlink will abide by any formal decision of the applicable data protection authority on any issues related to the interpretation and application of the BCPR where a right to appeal is not exercised.

6 UPDATE PROCEDURE

6.1.1 Approach

Seedlink will inform the national data protection authority, AP commissioner and any other relevant European data protection authorities of any change to the BCPR. Seedlink will provide that information within a reasonable time of the changes being made. The Seedlink EU Main Establishment is responsible for communicating changes to the BCPR and will also provide a brief explanation of the reasons for any notified changes to the BCPR.

However, Seedlink is not obliged to communicate changes to the BCPR which are administrative in nature or which have occurred because of a change of applicable data protection law in any European country through any legislative, court or supervisory authority measure unless they:

- result in a substantial change to the BCPR; or
- affect the authorisation of the BCPR by European data protection authorities. The Seedlink EU Main Establishment will maintain an up to date list of the Seedlink companies bound by the BCPR.
- Seedlink will send an up to date list of companies to the national data protection authority, AP commissioner and any other relevant European data protection authorities at least once a year

6.1.2 Communicating changes to Seedlink SCL and Individuals

Seedlink will communicate the amended BCPR to the Seedlink companies bound by the BCPR and will publish the amended BCPR on Seedlink's external web site accessible at www.seedlinktech.com.

The BCPR contain a change log which sets out the revision history of the BCPR, including the date the BCPR were revised and the details of any revisions made.

6.1.3 Inclusion of new Seedlink locations

Seedlink will ensure that all new Seedlink companies are considered for inclusion in the list of Seedlink companies bound by the BCPR and the T&C and SPP. Seedlink will also ensure that the necessary legal, administrative, operational and technical measures are in place before a transfer of personal identifiable information to or from a new Seedlink company takes place.

7 APPENDIX I IRT Team and Roles

Role/Business Area	Main Role Holder	Deputy
Team Leader	VP of IT & Security	CEO
Team Assistant Lead	Information Security Manager	CTO
Information Technology	VP of IT & Security	IT Specialist
Business Operations	CCO	CRO
Human Resources	HR Manager	Operations Manager
Communications (PR & Media Relations)	VP of Marketing	Director of Marketing

Roles and Responsibilities
The responsibilities of the roles within the incident response team are as follows:

Team Leader

- Decides if to initiate a response
- Assembles the incident response team
- Overall management of the incident response team
- Acts as interface with the board and other high-level stakeholders
- Final decision maker in cases of disagreement
- Assesses the risk to life and limb of the incident
- Considers environmental issues with respect to the incident
- Provide advice on business continuity options
- Invoke business continuity plans if required

Team Assistant Lead

- Supports the incident response team
- Co-ordinates resources within the command centre
- Prepares for meetings and takes record of actions and decisions
- Briefs team members on latest status on their return to the command centre
- Facilitates communication via email, telephone or other methods
- Monitors external information feeds such as news
- Attends the site of the incident as quickly as possible
- Assesses the extent and impact of the incident
- Provides first-person account of the situation to the IRT
- Liaises with the IRT on an on-going basis to provide updates and answer any questions required for decision-making by the IRT
- Deals with aspects of physical security and access
- Provides security presence if required

Information Technology

- Provides input on technology-related issues
- Assists with impact assessment

Business Operations

- Contributes to decision-making based on knowledge of business operations, products and services
- Briefs other members of the team on operational issues
- Helps to assess likely impact on customers of the organization

Human Resources

- Assesses and advises on HR policy and employment contract matters
- Represents the interests of organization employees
- Advises on capability and disciplinary issues
- Ensures that legal responsibilities for health and safety are met always
- Liaises with emergency services such as police, fire and medical

Communications (PR and Media Relations)

- Responsible for ensuring internal communications are effective
- Decides the level, frequency and content of communications with external parties such as the media
- Defines approach to keeping affected parties informed e.g. customers, shareholders
- Legal and Regulatory
- Advises on what must be done to ensure compliance with relevant laws and regulatory frameworks
- Assesses the actual and potential legal implications of the incident and subsequent actions

8 APPENDIX II Acronyms

Binding Corporate Privacy Rules	BCPR
Seedlink Corporate Locations	SCL
General Data Protection Regulation	GDPR
European Union	EU
Information Security Manager	ISM
Autoriteit Persoonsgegevens	AP
Artificial Intelligence	A.I.
China	CN
United States of America	USA
Information Security Management System	ISMS
Incident Response Team	IRT
Chief Executive Officer	CEO
Public Relations	PR
Chief Technical Officer	CTO
Terms & Conditions	T&C
Seedlink Privacy Policy	SPP
EU Main Establishment	EU LSA
Datacenter	DC
International Organization for Standardization	ISO
International Electrotechnical Commission	IEC
Information Technology	IT
One Time Password	OTP
Personal Identifiable Information	PII
Personal Data = Personal Identifiable Information	PII