Privacy Terms and Conditions: Corporate customers

These Privacy Terms and Conditions (hereinafter the "Terms") apply to the processing of personal data by Síminn hf. (hereinafter referred to as „Síminn", „Processor" or „Company") in relation to certain services Síminn may provide to its corporate customers (also referred to as „Controller"). In the course of providing any of these services to Customers, Síminn will act as a Processor on behalf of a Customer who is regarded as the Controller of the processing according to the Icelandic Act no. 90/2018 on Data Protection and the Processing of Personal Data (herein after referred to as „the Privacy Act").

In the event of discrepancy between the Icelandic and English version of these terms, the Icelandic version shall always prevail.

These Terms address the obligations of the Processor on behalf of the Controller, in relation to the processing activities of the services which these Terms apply to and are the equivalent to a data processing agreement („DPA"), cf. Art. 25, par. 3, of the Privacy Act.

Síminn may also resell services or third-party licenses to its customers. Such third parties may act as independent processors on behalf of the Controller according to the Privacy Act, without Síminn's involvement. This may apply in cases where the Controller obtains a software license from a third-party who simultaneously stores the Controller´s personal data.

It should be noted that these Terms only apply to the service that the customer purchases according to the its current Service Agreement with Síminn.

1. Subject matter of the processing

The Controller may purchase one or more of the corporate services that Síminn offers. Appendix 1 contains a description of the processing of personal data that Síminn processes in relation to each and every service in which Síminn is the Processor on behalf of the customer. These Terms apply whether a customer buys on or more of the corporate services specified in Appendix 1.

If a customer does not purchase any of the services specified in Appendix 1 Síminn does not process personal data as a data processor on behalf of the customer according to the Privacy Act. Specific conditions may apply concerning the sercive „Snjallari Bílar" (a vehicle tracking service), according to the terms of that particular service.

2. Controller´s obligations

The Controller declares that he is authorized to process the personal data that he entrusts the Processor to work with according to these Terms.

3. The Processor´s obligations

3.1. Confidentiality and training of employees

The Processor shall ensure the confidentiality of all data which the Processor may receive from the Controller, as well as any data which the Processor may become aware of in relation to his work as a service provider for the Controller and a Processor on behalf of the Controller. The confidentiality applies to information about the Controller's employees, customers, clients and other relevant parties. The confidentiality does not apply to information that has been made available to the public in accordance with law, or on the basis of a court ruling or ruling of a public authority in accordance with law.

The Processor shall ensure that his employees, which have been authorized access to and/or will handle data from the Controller according to these Terms, are bound by confidentiality in form of a written declaration (e.g. in employment contract) before they are authorized access to the data of the

Controller. Such confidentiality shall remain after the employee´s termination of employment with the Processor.

The Processor shall ensure that all employees, who have access to data from the Controller, have received appropriate training on the laws relating to the Processors' duties according to the processing of personal data.

3.2. Use of personal data

The Processor is aware that his employees may only process the personal data according to the purpose of the processing according to the Service Agreement, these Terms or the Controller´s instructions, unless otherwise stated in law. The Processor shall ensure that its employees only process the personal data according to these Terms and the Controller's instructions.

The Processor is prohibited from providing a third-party with access to any personal data, whether in writing og verbally, without the explicit consent of the Controller, cf. however Art. 5. The foregoing also applies to any service providers or contractors on behalf of the Processor, cf. however also Art. 8 of these Terms.

4. Security of personal data

a) General safety measures by the Processor

The Processor shall maintain appropriate technical and organizational measures to ensure adequate confidentiality of the personal data and to protect them against unlawful destruction, against accidental loss or alteration, and against unauthorized access, and/or any other unlawful processing. The measures shall take account the state of the art, the cost of implementation and the nature, scope, context and purpose and the risks of the processing.

In order to ensure appropriate technical measures, the Processor shall

a. be able to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services,

b. be able to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident,

c. implement a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing, and

d. use pseudonymisation and encryption of personal data, where applicable.

In assessing the appropriate level of security, account shall be taken to the risks that are presented by processing, in particular from accidental or unlawful destruction, against accidental loss or alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.

The Processor must conduct effective internal controls to ensure compliance with the safety measures of the company, e.g. by implementing audits. For example, the Processor must ensure that only those employees of the Processor who necessary need access to the personal data to perform their duties/services shall have appropriate access to those systems and that internal controls maintain correct and appropriate access of employees.

The Processor shall ensure that his company complies with the Icelandic Data Protection Authority´s rules no. 299/2001 on the security of personal data and that the company´s activities are certified according to the ISO 27001 standard on information security. The Processor should inter alia ensure the physical security of his premises and the security of data and software/data

centers/servers/copying systems/information systems and portable storage media (e.g. with appropriate antivirus, access controls, and logins).

The Processor shall, on the request from the Controller, assist the Controller in conducting a data protection impact assessment, in cooperation with the Controller.

b) Personal data breach and notification obligation

The Processor shall notify the Controller without undue delay after becoming aware of a personal data breach.

The notification shall include information or a description of the nature of the personal data breach including the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned. The Processor shall also describe the likely consequences of the personal data breach and the measures taken or proposed to be taken to address the personal data breach. All documents and data necessary for the Controller to notify the breach to the relevant data protection authority shall be included in the notification, where the Processor has such documents and data.

If a Controller notifies a personal data breach concerning the Processor to the Icelandic Data Protection Authority, the Controller shall keep the Processor informed of the proceedings with the Authority, incl. providing the Processor with a copy of the notification sent to the Icelandic Data Protection Authority, where applicable.

c) Special safety instructions from the Controller

Where the Controller considers it necessary to give the Processor further instructions on specific security measures related to the nature, scope and type of the processing, any such instructions shall be sent to the Processor‘s contact for review and approval.

5. Access to personal data

The Processor shall ensure that the Controller can monitor the compliance of the Processor with the provisions of these Terms and the Privacy Act, e.g. by providing the Controller with enough information and/or data upon request.

The Processor shall enable the Controller to conduct, or deploy a third-party to conduct on its behalf, audits on the Processor’s processing of personal data and provide appropriate assistance in conducting such audits. The purpose of such audits is to make sure that the Processor fulfills its obligations laid down in these Terms and the Privacy Act.

The Processor shall ensure that personal data is available to supervisory authorities for their possible audits and/or for the surveillance activities of such entities. If a supervisory authority requests access to the personal data of the Controller based on an explicit authorization or a court order, the Processor shall notify the Controller as soon as possible, preferably before such access is granted, unless such disclosure is prohibited. The access of authorities could also include access to premises and employees of the Processor. In such cases, the Processor shall inform the Controller of the disclosure of personal data and/or the information relating to the Processor´s role according to these Terms soon as possible, incl. which supervisory authority requested access to data, what was the scope of the request, what legal basis the request was based on, what information was provided and by what means, as far as permitted.

If the Processor is in doubt as to whether to provide access to or provide personal data according to the foregoing, he shall seek advice from the Controller at the earliest opportunity and before access is provided, as far as permitted.

Also, the compliance officer of the Controller, as well as external and/or internal auditors of the Controller and its security officer shall be provided access to all data provided by the Controller and the Processor hosts and/or processes according to these Terms, where appropriate and for the purpose of examining the performance of the Processor´s services on behalf of the Controller according to these Terms or the Service Agreement.

The Processor is prohibited from transferring the personal data outside the European Economic Area (EEA) unless instructed to do so by the Controller, cf. also Art. 8.

6. Data subject´s rights

The Processor shall assist the Controller by appropriate technical and organizational measures to the extent possible and with regard to the nature of the processing, to respond to requests for exercising the data subject's rights in accordance with the Privacy Act and other relevant rules on data protection, e.g. access to personal data, information on processing, rectification or erasure of data, right to object to processing, limitation of processing, destruction of data and portability of data. Síminn reserves the right to demand a service charge related to the requests with respect to the scope and nauture of requests at any given time.

If the Processor receives a request from an individual based to the Data Subject rights according to Privacy Act, the Processor shall advise the person concerned to turn to the Controller if information about the person is contained in the personal data processed by the Processor according to the Service Agreement and/or these Terms or forward any such requests to the Controller's contact person. The Processor shall not answer requests from the data subjects without the consent of the Controller.

7. Return or deletion of personal data

The Processor shall, in consult with the Controller, erase the personal data where the data is no longer necessary in relation to the purpose for which they were collected, unless otherwise required by law.

The Processor must return or delete all the personal data, incl. possible copies of them, when written instructions in that regard are received from the Controller, and never later then on termination of the Service Agreement unless otherwise required by law.

The foregoing concerns information in any format, whether on paper, in electronic form or in any medium related to the service of the Processor to the Controller. The Processor shall confirm the return of data to the Controller or certify the safe deletion of the data in writing to the contact person of the Controller if requested by the Controller. Safe deletion of data is considered e.g. deletion by an AAA-certified party specialized in data deletion.

8. Use of sub-processors etc.

The Processor may assign rights or obligations according to the processing of personal data covered by these Terms to third parties, e.g. to sub-processors, either in full or in part.

Appendix 2 contains a list of the sub-processors and the description of the processing engaged by them on behalf of the Processor. By agreeing to the Terms, the Controller approves the sub-processors on behalf of the Processor mentioned therein.

The Processor also reserves the right to add sub-processors. Prior to such an amendment, the Processor will send a notice to the Controller where the Controller is granted five (5) business days to object to the sub-processor(s) in question. If no objection is received by the Processor within the time limit, he may engage the sub-processor concerned.

If the Processor stops using a specific sub-processor, the Processor shall inform the thereof with a written notification where possible.

The Processor shall i.a. ensure that the sub-processors comply with the same privacy obligations as set forth in these Terms. The Processor is responsible if the sub-processors fail to comply with their obligations.

Nothing in these Terms shall be interpreted as meaning that the Processor acquires ownership or irreversible use of such data, incl. the personal data provided by the Controller according to these Terms or Service Agreement or arising from the processing of data according to those services.

9. Assignment

Except as otherwise provided in these Terms, the Processor may not assign rights or obligations according to these Terms to third parties except with the written consent of the Controller.

10. Liability

All matters concerning liability and limitations thereof concerning any breaches to these Terms shall be governed by liability clauses in the Service Agreement. Any liabilities concerning possible violations of the Privacy Act are subject to the provisions of that Act.

11. Duration and termination

These Terms take effect on the date of publishing. They shall then enter into force *vis-á-vis* the Controller whenever he agrees to the Terms or as soon as he begins to use the service of the Processor, specified in Appendix 1. The Terms remain in force while the Service Agreement between the Parties is valid or while the Controller purchases corporate services from the Processor which are covered by these Terms.

In the event, that the Processor starts to use a sub-processor that the Controller has demonstrably objected, in accordance with Art. 8 of these Terms, the Controller has the right to terminate the relevant service, cf. Appenidx 1, within two months from receiving notification thereof. Termination shall take effect as soon as it is received by Síminn.

Should the Controller not accept amendments to these Terms made by the Processor, cf. also Art. 13, the Controller may terminate the relevant service specified in Appendix 1 with 30 days' notice, within one month of the notification of the amended Terms.

The Controller´s right to terminate services according to these Terms shall prevail over any termination conditions specified in the Service Agreement between the Parties.

12. Jurisdiction

These Terms shall prevail over other agreements in relation to the Processor´s processing of personal data and other related obligations. However, if the Parties have signed a specific Data Processing Agreement, such an agreement shall prevail over these Terms.

These Terms are governed by Icelandic law, in particular Act no. 90/2018 on Data Protection and Processing of Personal Data. Should a dispute arise concerning these Terms, the parties shall bring the matter before the District Court of Reykjavík.

13. Review

Síminn reserves the right to amend these Terms in accordance with changes to applicable laws and/or regulations or due to changes related to the processing operations by the Processor. If any changes are made to these Terms, corporate customers will be notified at least one month before the new Terms take effect.

However, this does not apply to amendments to Appendix 1 which can occur when the Processor adds new services that are subject to these Terms. In such cases, the amendments shall take effect on the date they are published.

The same applies to amendments to Appendix 2 which contains a list of the sub-processors used by the Processor, cf. Art. 8 in these Terms.

Any amendments to these Terms will take effect when the updated version of the Terms has been published on Síminn's corporate customer service-web („*Þjónustuvefur fyrirtækja*").

APPENDIX 1

SERVICES SUBJECT TO THE PRIVACY TERMS AND CONDITIONS

This Appendix specifies the services that are offered to Síminn's corporate customers where Síminn processes personal data on behalf of the customers within the meaning of the Privacy Act, as further defined in the Privacy Terms and Conditions.

A customer may purchase one or more of the following services. The description of the data processing activities in relation to each service therefore applies to the customer as appropriate.

For each individual service it is described what personal data Síminn processes on behalf of the customer. However, it should also be noted that in relation to the services, the customer may also request assistance from Síminn's Servicedesk, and in connection with such assistance, Síminn's specialists may be granted access to the customer's systems or solutions where personal data can be stored.

Further processing of personal data by Síminn in connection with the following services is only carried out on the basis of written instructions from the customer, as applicable.

DESCRIPTION OF THE SERVICES

1.1. *Símavist*

In order to provide *Símavist* Síminn processes the following data:

- name of the beneficiary that purchases the services, phone numbers, email addresses, name of phone numbers' users, attendances, call transfer data, call log (last 20 answered calls, missed and dialed calls regardless of time for all users) call center data (call log of all incoming and outgoing calls) and call center login data.

Síminn may also, as applicable, have access to personal data when installing a system at the customer's site, and in addition all data collected by the use of the system is hosted by Síminn.

In relation to installation and connections, Síminn will also receive data on the users for specified numbers, that is numbers which belong to certain employees or other persons related to the customer.

Síminn's Terms and Conditions, Síminn „Símavist_Tilboð", contain the terms applicable for this service.

1.2. Call recording

In order to provide *Call recording* services Síminn processes the following data:

- name of the beneficiary that purchases the service, phone numbers that are being recorded, name of phone numbers users and administrator access (username and password), logins and activity-logs in the system.

Síminn provides technical support and installation services, and hosts and stores calls that the customer chooses to record. Accordingly, Síminn thus also processes call content on behalf of the customer.

Síminn's Terms and Conditions, Síminn „Símavist_Tilboð", contain the terms applicable for this service.

1.3. Bulk text messages

In order to provide *Bulk text messages* services Síminn processes the following data:

- name, social security number and e-mail address for users/additional users, as well as data on the users' usage of the services, such as contact information, groups, phone numbers which messages are sent to, timing as well as billing information.

The service gives the customer access to a website where the customer fills in data, such as, recipients' phone numbers and the text the customer decides to send. The customer can also create groups of recipients with the solution. This data collected by the use of the services is stored in Síminn's system and the services thus include hosting services. It shall be noted that the content of text messages is not stored by Síminn.

It should also be noted that the transmission of the message itself is considered part of Síminn's telecommunication service which is not covered by these Terms. The Terms and Conditions for „Bulk text messages" can be found here; https://www.siminn.is/forsida/adstod/skilmalar.

1.4. Mail services

It shall be stated that Síminn **does not** service the mail service for Office365 and the Privacy Terms and Conditions do thus not apply to such mail hosting.

a) Mail hosting

In relation to mail hosting services Síminn provides technical assistance to customers in creating, modifying and/or closing email accounts. Síminn can also carry out troubleshooting in relation to problems concerning accounts. If a user has forgotten a password to access his account, Síminn can provide the user with a temporary password and/or reset the account password as appropriate.

When providing the services, a customer may provide Síminn access to an account or login information related to a particular account, either by telephone or in writing.

In order to provide mail-hosting services, Síminn will process the following data:

- customer accounts (including for the customer's employees), the employees' email addresses which are connected to the accounts, log-in information (including temporary passwords and IP addresses behind logins).

The accounts and related data are hosted in Síminn's mail service network in Iceland. Síminn uses the data to provide the customer the account related services, in particular in relation to troubleshooting, to create, modify or close an account, or to restore passwords for an account, as applicable. Information on customers' passwords to an account is not stored by Síminn.

b) Mail filtering

In relation to mail filtering, Síminn's services include the filtering of all emails which are received by or sent to the customer's defined email addresses for the purpose of decreasing and preventing the circulation of spam and email viruses in the customer's mailbox. Síminn further provides the customer with support and troubleshooting services in relation to the mail filtering features.

Siminn will process the following personal data in relation to the mail filtering services:

- number of emails received by and sent from the customer and mail metadata (including date and timing, size, whether the email includes an attachment (yes/no) and if so name of the attachment, title of mail, email address of sender and recipient, IP-address of sender's mail server), error message code, where applicable, and whether the email has been stopped

(delayed or sent back) and if the email has been stopped the content of the email may be accessible.

The above data which is collected in relation to the services are stored on a mail server in Iceland. Síminn has access to the data for the purpose of providing the customer with the services, in particular for troubleshooting purposes. The data is kept for six months in accordance with the requirements of the Icelandic Electronic Communication Act.

1.5. Domain hosting

a) DNS hosting

Síminn is a hosting provider and undertakes to create and block DNS hosting on a domain. Síminn also provides customers services related to the configuration and changes of DNS records.

In order to provide *DNS hosting on a domain* services Síminn will process the following data:

- IP address behind a domain registration on a DNS server.

The data is hosted on Síminn‘s DNS servers in Iceland, but Síminn will not review the data unless requested by the customer, such as in order to provide technical support.

b) Web hosting

Síminn is a web hosting provider and undertakes to create and block domains. Síminn can also provide customers services related to the configuration and changes of DNS records.

In order to provide *web hosting on a domain* services Síminn will process the following data:

- IP addresses behind site entries
- Síminn also has access to personal data that the customer has uploaded to his own site.

The data is hosted on Síminn‘s web hosting servers in Iceland, but Síminn will not review the data unless requested by the customer, such as in order to provide technical support.

1.6. Firewall service

The firewall service entails that Síminn installs firewall and associated antivirus protection to be able to monitor all traffic passing through Síminn‘s equipment on a customer‘s local network. The purpose of the monitoring is to monitor the quality and security of the customer‘s online services, as well as to detect and respond to faults or unexpected load (for example, because of a virus) as appropriate in consultation with the customer.

In order to provide the *firewall service* Síminn processes the following data:

- IP addresses that may be collected for monitoring purposes, for example those who access websites which the customer has defined as a high risk. The IP addresses may be related to employees or other persons connected to the customer’s network equipment.
- Device identifier associated with customer‘s network equipment, if such identifier carries personal data.

Síminn collects and stores the data for the purpose of setting up and providing the services to the customer. The data is hosted on Síminn‘s equipment in Iceland.

APPENDIX 2

USE OF SUB-PROCESSORS

In accordance with the Privacy Terms and Conditions, the Processor may entrust specified third parties, so-called *sub-processors*, to carry out all or part of the data processing activities that the Processor undertakes on behalf of the Controller.

The Processor reserves the right to use the services of the following sub-processors to perform the following processing activities:

Símavist:

BroadSoft Inc. (Cisco Systems Inc.)
170 West Tasman Drive
San Jose, California 95134
https://www.broadsoft.com/

In relation to the installation of services Síminn uses the Broadworks cloud solution from its processor Broadsoft (a subsidiary of Cisco) in the United States. All data is hosted by Síminn in Iceland, but when necessary Síminn provides Broadsoft with access to data for the purpose of solving technical problems. Upon granting such access, data could be provided to Broadsoft on the basis of a processing agreement between Síminn and Broadsoft. Transfer of data to the United States is based on Standard Contractual Clauses from the European Commission.

Call Recording:

Sensa ehf.
Ármúla 31
108 Reykjavík, Ísland
https://sensa.is/

Sensa‘s processing involves the hosting of the system and all the data collected.

Bulk Text Messages:

Miracle ehf.
Kringlunni 7
103 Reykjavík, Ísland
http://www.miracle.is/

Miracle‘s processing involves creating backups and analyzing software layer errors.

Mail Services:

Sensa ehf.
Ármúla 31
108 Reykjavík, Ísland
https://sensa.is/

a) Mail hosting
Sensa‘s processing involves hosting and operating the mailbox servers. Sensa also provides Síminn with technical support in special circumstances and may therefore also have access to the login information that a customer may have provided to Síminn, as well as the mailbox itself.

b) Mail filtering

Sensa's processing involves the hosting and operating of servers where the data which is collected via mail filtering (incl. spam filtering). Sensa provides Siminn with technical support in special circumstances, such as regarding troubleshooting and customer services.

Domain Hosting (DNS and Web Hosting):

Sensa ehf.
Ármúla 31
108 Reykjavík, Ísland
https://sensa.is/

Sensa's processing involves hosting and operation of the DNS servers. In addition, Sensa may provide Síminn with technical support, such as in relation to installation, modification, changes to a certain webpage and/or a transfer of a page to a new hosting service. In relation to such work, Sensa may also gain access to the same data as Síminn.

Firewall Service:

Sensa ehf.
Ármúla 31
108 Reykjavík, Ísland
https://sensa.is/

Sensa may obtain access to data collected through the equipment for the purpose of providing Síminn with technical assistance upon request. All data is stored on Síminn's equipment by Síminn in Iceland.

Síminn Servicedesk:

Sensa ehf.
Ármúla 31
108 Reykjavík, Ísland
https://sensa.is/

Sensa may obtain access to customer data when Síminn requests technical assistance from Sensa.