ipnordic

DATA PROCESSING HANDBOOK

Version: 1.0

Status: Approved

Date:Februar 2021

Configuration

Distribution management

Version	Date	Description
1.0	Februar 2021	First edition of the Data Processing Handbook

Approval

Name	Position	Date
Charles Ginnerskov	CEO	Februar 2021

Contents

1 Definitions

The terms used in this handbook are defined as follows. The definitions of the most important terms are based on the definitions used in the General Data Protection Regulation ("**GDPR**"):

"Customers": The party to whom we supply our services concluded with us, under the ipnordic Terms of Service, found on the order conformation.

"**Data Breach**": An accidental or unlawful breach of security leading to the destruction, loss, alteration, or unauthorised disclosure of, or access to, personal data that has been transmitted, stored, or otherwise processed.

"**Third Party**": A natural or legal person, public authority, agency or body other than the Data Subject, Data Controller, Data Processor, or persons who, under the direct authority of the Data Controller or Data Processor, have been authorised to Process Personal Data.

"Us", "We", "Our", "us", "we", "our" "ipn" "ipnordic": ipnordic A/S and other Enreach Group level recipients described in **Appendix B**.

"Communicator": The software and online portal of ipnordic which you can use to manage the delivery of your services.

"**Personal Data**": any information relating to an identified or identifiable natural person (the "**Data Subject**"); a natural person is identifiable if they can be directly or indirectly identified, in particular using an identifier such as a name, an identification number, location details, an online identifier, or using one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

"**Sub-Data Processor**": A party that processes Personal Data for the Data Controller under contract to a Data Processor.

"**E-privacy directive**": National European Telecommunications Acts, including but not limited to the Danish Telecommunication Act derived from Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). This act will be revised at some time in the future in connection with the implementation of the (draft) Directive for the introduction of the European Code of Electronic Communication (COM 2016 (590)). In addition, the draft E-Privacy Regulation will also replace sections of the National European Telecommunications Acts.

"**Consent**" **of the Data Subject**: Any freely given, specific, informed, and unambiguous indication of the Data Subject's wishes whereby the Data Subject, by a statement or by a clear affirmative action, signifies agreement to the Processing of Personal Data relating to him/her.

"You", "Your", "you", "your": A customer who buys one or more services under an agreement with us;

"**Processing**" **or** "**Process**": Any operation or set of operations that is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

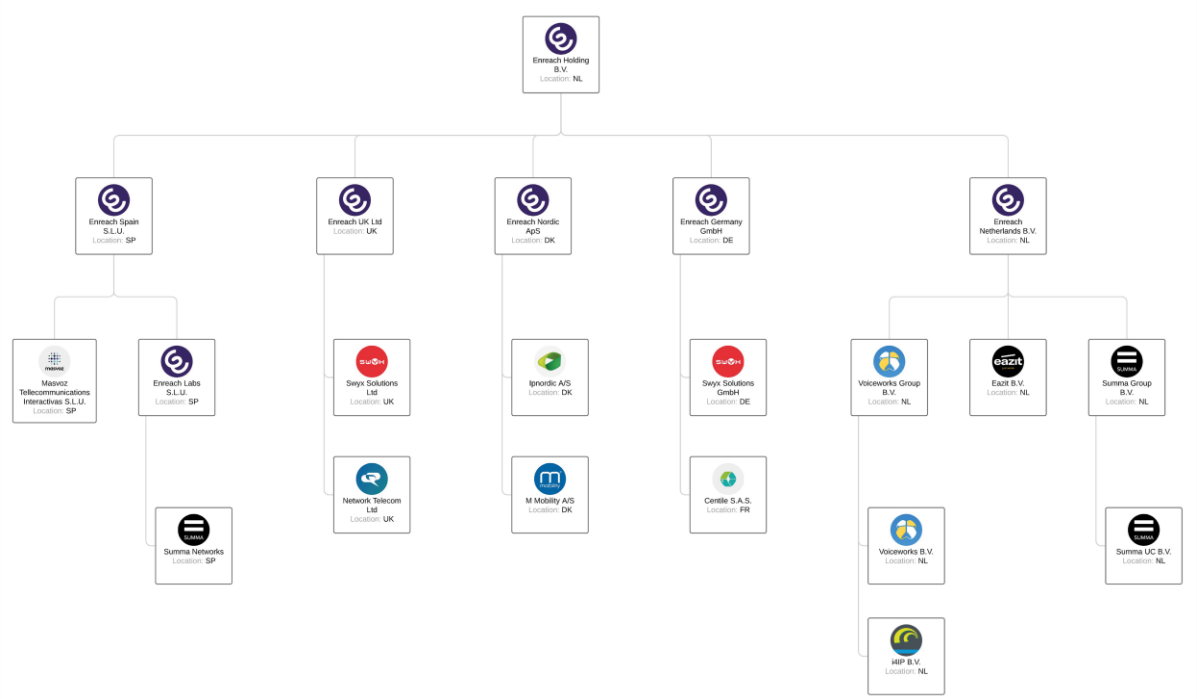
"**Data Controller**": A legal person that determines the purpose and means of the Processing of the Personal Data.

"**Data Processor**": A natural or legal person that processes Personal Data on behalf of the Data Controller.

2 What is this handbook for?

2.1 Introduction

As a telecommunication company we know that data protection is important. We also understand and expect that some of our Customers do not have the ressources availeble to thourougly understand the complexity of the obligations imposed by the GDPR regarding to the delivery of telecommunication solutions. Therefore in the spirit of ipnordic´s DNA, namely providing great customer service to our customers and making B2B telecommunication solutions easy, we will aim to explain this complexity in the most practical and operational way possible. We feel that this will give you, our beloved Customers, the best possible tools available, so that you can live up to the obligations, that you and us are obliged to comply with.



*The organization chart above is subject to adjustments, restructurering and changes and might therefore not precisely reflect the organizational structure of the Enreach Group.

ipnordic is part of the Enreach Group, a pan-european unified communications company. Enreach provides collaboration technology and telecom services through their reselling partners and direct brands, of which ipnordic is one. Above is a organizational chart describing the current Enreach Group Level entities and what nations they are established in.

We have made this handbook with the purpose of explaining, in a clear and transparent way, how we fulfil our obligations under the Danish Telecommunication Act and the GDPR in relation to the Processing of Personal Data. In particular, the handbook makes clear the obligations that might involve you as a Customer. We explain what we expect from you in our role as Data Controller, but also exactly what you can expect from us in our role as your Data Processor. In situations where ipnordic is acting in the role as Data Processor, this handbook will have the status of a Data Processing Agreement and is thus a binding contract as required under Article 28(3) of the GDPR. The contents of that agreement are described in more detail in Chapter 4 of this handbook.

As will be made clear in Chapter 4, we try to fulfil our Data Processor's obligations as practically and as concretely as possible. We believe that we can only provide a scalable, and competitively priced service if we, as a Data Processor, are able to serve our Customers in as far as possible in the same way. This means, for example: (i) we will report Data Breaches independently to the Data Protection Authority, but we will send you a copy of the notification and of course explain the remedial measures we will take to address the Data Breach, (ii). If we decide a data protection impact assessment needs to be carried out, then we will carry it out on your behalf and provide you with a copy of the report on the findings.

2.2 Contents of the handbook

First we have outlined the inventory of the services we offer and the "GDPR roles" that we have. This inventory is included in Appendix A of this handbook. Depending on whether or not we determine the purpose and means of the Processing of the relevant Personal Data, we are either the Data Controller or your Data Processor. The table in Appendix A also sets out which types of Personal Data we Process for each service and, if we are the Data Controller, for which purposes. The relevant purposes are indicated with a check mark.

This handbook only relates to our core network, and not the networks of the telecom providers that we use to facilitate the supply of our services to you. We mainly use the network of TDC, Hi3g and Telia for our services. If the services you have asked us to provide for you involves the Processing of Personal Data within the network of TDC, Hi3g, or Telia then we will be glad to pass on your request or to put you in touch with TDC, Hi3g or Telia directly. TDC, Hi3g and Telia has informed us that, independently from us, it is the Data Controller for the Processing of Personal Data in connection with the provision of its services. TDC, Hi3g and Telia are therefore not a Data Processor for us.

2.3 Integration with the Order Confirmation and the ipn Terms of Service

This handbook sets out both your and our rights and obligations. The handbook is integrated into the ipnordic Terms of Service(TOS) section 16, thus making it a integrated part of the delivery of our service to you. Like our previous Data Processing Agreement process, you accept our offer by paying for the service.

You are under no obligation to accept the content of this handbook and under the provisions of Article 28 GDPR, it is your own responsibility to conclude a Data Processor's Agreement with us. The decision is yours. However, this handbook is our only offer for such an agreement.

This handbook replaces our standard Data Processing Agreements (the one that have been available to you through our order confirmation and on our homepage). This also means that the current Data Processing Agreement that we have concluded with you beforehand for the services included in Appendix A, will only be valid until the 15.03.2021, if you by paying for our services, accept the offer included in this Data Processing Handbook.

If you have negotiated a non standard Data Protection Agreement with us, due to the fact we provide you with a special service, meaning a service not included in Appendix A, or you are under specific legal obligations, other than GDPR, that require that you have a special Data Proccessing Agreement, this Handbook will not override such a agreement. Please contact us directly at compliance@ipnordic.dk if you have questions about existing Data Processing Agreements.

2.4 Link with the privacy policy

This handbook does not replace our privacy policy. It is a separate document. If we are acting only as a Data Controller, then our external privacy policy applies instead of this Handbook.

2.5 Link to the order confirmation

The instruction for the processing of Personal Data in regards to the telecommunication services offered by ipnordic is provided to us in the order confirmation. Meaning, that if you have ordered a service from us, we will see that as an instruction to process the Personal Data required to provide the service ordered by you. If you go to Appendix A, you can see what types or Personal Data is used for the different services offered by ipnordic and whether we are a Data Processer and a Data Controller in regards to the processing of your Personal Data.

3 ipnordic as Data Controller

3.1 Introduction

Because you have direct contact with the Data Subjects, we need you to provide us with your cooperation in two areas. Without that cooperation we cannot fulfil our obligations as a Data Controller under The E-privacy directive and the GDPR. If, for example, obligations are imposed on us under statutory regulations, which we cannot fulfil without your or your end users cooperation , we will notify you about these obligations. In such cases, we need you to provide us with your immediate and full cooperation so that we are able to comply with these regulations, and if necessary also impose the applicable regulations on you (and indirectly your end users). The two areas where we need your cooperation are the obligation to provide information under Article 14 GDPR and the obligation to notify Data Breaches to Data Subjects. If you do not provide your full cooperation, then it is possible that we could be held liable by the Data Subjects. We will then have the right to take action against you to recover any damages that we suffer as a consequence.

3.2 Obligation to provide information

We process the Personal Data of Data Subjects, which we have no direct (contractual) relationship with. This is the Personal Data of the end users of our services, in most cases the end user will be your employees. We get this Personal Data from you. Because we do not receive the Personal Data directly from the Data Subjects, under Article 14 GDPR, as a Data Controller we have an obligation to provide the Data Subjects with the information described in Article 14 (1) and (2) GDPR. We have to do so within 1 month after we have received that data from you. Consequently, we will include the text of the relevant provisions in this handbooks Appendix C, which you can then include in your privacy statement. We expect you to communicate, or arrange the communication of, that statement to the relevant Data Subjects before you set up the connection to our service.

3.3 Notification of Data Breaches

3.3.1 Introduction

We are a provider of public electronic communication services. As such, we have a special obligation to report security breaches, as defined in § 8(2) of The Danish Telecommunication Act, which have adverse consequences for the protection of the Personal Data that is processed by us in connection with the provision of a public electronic communication service. In situations where we are the Data Controller, we will expect any Data Breach that affects Data Subjects to be a Data Breach that falls within the scope of § 8(2) of The Danish Telecommunication Act. Under Article 95 GDPR, we will then not be obligated to also comply with the general obligation to notify provided for under Article 33(1) GDPR.

3.3.2 The notification procedure

We have drawn up a procedure that enables us to detect, address, and report Data Breaches to the Data Protection Authority within the period prescribed under § 8(2) of The Danish Telecommunication Act. Our starting point is that any Data Breach that meets the criteria for notification set out in § 8(2) of The Danish Telecommunication Act will always be reported to the Data Protection Authority. If we are required to notify a Data Breach to “your” Data Subjects under § 8(2) of The Danish Telecommunication Act, we will inform you about this. We will send you the text of the notification that you will have to send to “your” Data Subjects within a reasonable period after the notification of the Data Breach, to the Data Protection Authority. We will expect you to then send out this notification without making any changes.

If we report a Data Breach related to Persona Data of “your” Data Subjects, we will notify you about this by e-mail, We will not send this e-mail beforehand if it is not reasonably possible due to the need for urgent action. In that case, we will send the e-mail as quickly as possible after the notification has been made.

4 ipnordic as Data Processor

4.1 Introduction

In this chapter, we describe how we, as a Data Processor, will comply with the requirements of the GDPR. We have described the Personal Data that we process for you and the categories of Data Subjects to which the Personal Data relates, in **Appendix A**. We Process all Personal Data for the duration of the agreement that we have concluded with you, and only so we can provide the agreed services. All employees, consultants, and suppliers that Process personal data on our behalf are contractually obligated by us to handle the personal data confidentially.

4.2 Group level processing activities

Most of the services described in **Appendix A** are operated by ipnordic, and are processed in Denmark and within our core network. Some services offered by us are provided by other Enreach Group entities and processed within their core network in the countries where they are established. An overview of all group level recipients of your Personal Data in our role as a Data Processor are made available in **Appendix B** under Approved faclities. All group level recipients are subject to internal policies and procedures specifying that they must follow the decisions and instructions of the the Data Controller and are subject to the same security obligations, as described in 4.8 of this chapter.

4.3 Instructions

Article 29 of the GDPR stipulates, that as a Data Processor we have to Process Personal Data exclusively in accordance with your instructions. Our starting point is that your instructions have been exhaustively described in this handbook. If you want to give us instructions that are not described in this handbook, then we will be entitled to see these instructions as an order given by you to us for the performance of specific activities for a certain fee. We will schedule the performance of the order for you if we have sufficient capacity for such. We will only be obligated to carry out the order if you have accepted the order confirmation.

Notwithstanding the foregoing, we will comply with all applicable laws and regulations in Denmark concerning the Processing of Personal Data, and we will act in accordance with what is promised in this handbook. If you give us instructions that in our opinion are in contravention of the GDPR or other applicable data protection laws and regulations, then we will notify you about this immediately in writing.

In certain situations, in order to comply with national laws and regulations, we might have to Process Personal Data contrary to your instructions, for example if we have to disclose Personal Data to comply with the order of an official authority. If we have to do this, we will notify you about it in advance , unless the relevant regulations prohibit us from doing so.

4.4 Sub-Data Processors

4.4.1 Introduction

We have drawn up a list of our data processors which you can contact via **Appendix B**. They are the suppliers we use to supply our services to you. These suppliers Process the Personal Data of end customers. We always conclude a Data Processor's Agreement with our data processors, which imposes the same obligations on the sub-data processors as those imposed on us under this handbook.

4.4.2 Existing services

We assume that in general you will allow us to use the data processors included in **Appendix B**. If the list of data processors changes, then we will inform you about this at least one month in advance. You can object to a change. After this objection has been received, we will meet with you and hear your objections. However, we would like to point out that if we are unable to agree on a solution for your objection, then the only consequence of your objection will be that we will allow you to cancel the relevant service.

4.4.3 New services

We will inform you in advance about new services that we are developing and/or if sub-data processors will be used for these services. You can decide for yourself if you want to use these new services. We are allowed to have personal data Processed by sub-data processors who are established in a country outside the European Economic Area (**EEA**) in connection with new services without your Consent.

If sub-data processors are established outside the EEA, and the country where the sub-data processor is established does not offer an adequate level of protection in the sense of Article 45 (1) GDPR, then we will make sure that the relevant sub-data processor only receives Personal Data from us if the appropriate safeguards have been provided as required under Article 46 (2) GDPR. At this point in time, that means we will conclude an agreement with the relevant sub-data processor based on so-called "EU model contracts for the transfer of personal data" (EU decision 2010/87/EU) or, if the sub-data processor is established in the United States of America, the sub-data processor is certified under the EU-US privacy shield agreements.

4.5 Rights of Data Subjects

4.5.1 Introduction

As a Data Controller, under the GDPR you have to give Data Subjects the opportunity to exercise their rights as provided for in Chapter 3 of the GDPR, and specifically the right to access their Personal Data (hereafter called "**Access Rights**"). Access Rights give Data Subjects the right to do certain things with their Personal Data or to restrict the Processing of that Personal Data.

Because we Process Personal Data of Data Subjects which you have contact with, we have to offer you access to the Personal Data of "your" Data Subjects within our core network, and make it possible for you to modify, erase, or export that Personal Data to another provider. We will describe how we will make this possible for you in section 4.4.

You cannot erase data that we need in order to operate the service. If you modify or erase data, then you will be liable for any adverse (financial) consequences of any mistakes you make when you do this. We cannot be held liable for any errors in data modified by you. We also expect that any modifying or erasure of data will always be carried out by you with the direct or indirect Consent of the Data Subjects. If that is not the case, then you will be obligated to indemnify us against any claims of the relevant Data Subjects.

4.5.2 The Access Rights

Below, We have drawn up a summary of the Access Rights which you might have to deal with in connection with the provision of our services. For each right, we explain how you can facilitate the exercise of that right. This is described in the column "How?". This is the only way we will enable you to give "your" Data Subjects the opportunity to exercise their rights as provided for under Chapter 3 of the GDPR. ipnordic´s Support e-mail and main number, are always available at www.ipnordic.dk.

As described in the article 12(6) of the GDPR– If we as the Data Controller have reasonable doubt to the identity of the Data Subject requesting the use of The Rights of the Individual, we may request additional information that we deem necessary to confirm the identity of the data subject. As you are the entity that has direct contact with the Data Subject, we may ask you to help us confirm the identity of the individual seeking access.

The right	Your action	How?
Right of access (Articles 12, 15 GDPR).	Issuing a copy of the data in a standard file format.	You view/download the data from Communicator, ipoffice, our online portal or you contact support.
Right to rectification (Article 16 GDPR).	Rectification, completion, or removal of data.	You modify the data in Communicator, ipoffice, you contact support or you delete the data from Communicator
Right to erasure ("Right to be forgotten") (Article 17 GDPR).	Erasure of data.	You delete the data from Communicator or you contact support. If a telephone number is published in a directory or online, then you have to arrange the deletion of it yourself.
Right to restriction of Processing (Article 18 GDPR).	Not relevant for our services.	Not relevant for our services.
Right to data portability (Article 20 GDPR)[1].	Download and export data from our core network.	You download the data from Communicator or you contact support.
Right to object to the Processing (21(1) GDPR).	Not relevant for our services.	Not relevant for our services.

4.6 Notification of Data Breaches

4.6.1 Introduction

We are a provider of public electronic communication services. As such, we have a special obligation to report security breaches, as defined in § 8(2) of The Danish Telecommunication Act, which have adverse consequences for the protection of the Personal Data that is processed by us in connection with the provision of a public electronic communication service. In addition to usas a Data Processor we have to enable you to comply with the general obligation to notify provided for under Article 33(1) GDPR. We will describe the procedure we follow for Data Breaches in the context of the relationship we have with you as the Data Processor of Personal Data in this section 4.5.

4.6.2 The notification procedure

We have outlined a procedure that enables us to detect, address, and report Data Breaches to the Data Protection Authority within the period prescribed for such under §8(2) of The Danish Telecommunication Act and/or the GDPR (Article 33(1) GDPR).

Our starting point is that we will always independently report any Data Breach that meets the criteria for reporting set out in §8(2) of The Danish Telecommunication Act to the Data Protection Authority within the periods prescribed by law. The obligation to report under article §8(2) of The Danish Telecommunication Act is a special obligation to report, and applies in addition to the general obligation to report under article 33(1) GDPR. If we are required to notify a Data Breach to your end users under Article §8(2) of The Danish Telecommunication Act, we will inform you about this. We will send you the text of the notification that you will have to send to your end users within a reasonable period after the notification of the Data Breach to the Data Protection Authority. We expect you to make this notification availeble without making any changes.

[1] EDPB (Article 29 Working Party): Guidelines for the right to data portability (https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/richtlijnen_dataportabiliteit.pdf).

If a Data Breach has to be reported under Article 33(1) GDPR, then we will report it on behalf of all our customers simultaneously. You authorise us a priori to do this. When we report a Data Breach, we will include a list of the Data Controllers which the notification relates to. If we report a Data Breach, we will notify you about this beforehand by e-mail provided the notification relates to Personal Data of your end users. We will not send this e-mail beforehand if it is not reasonably possible due to the need for urgent action. In that case, we will send the e-mail as quickly as possible after the notification has been made.

4.7 Data protection impact assessment

We are of the opinion that the services we provide, in any case as of 25 May 2018, are not of such a nature that you, as a Data Controller, are obligated to carry out a data protection impact assessment for these services. This is because the nature of the data that we Process is not likely to result in a high risk to the rights and freedoms of Data Subjects (Article 35, paragraph 1, GDPR). As substantiation for our standpoint, we refer to the list of the criteria that the European Data Protection Board (EDPB, formally the Article 29 Working Party) has drawn up for such[2]. Based on these criteria, our services do not involve Processing of Personal Data with a high risk. We trust that you concur with our assessment. A periodical review will be carried out to verify the validity of our standpoint. If this changes in the future, for example if we introduce a service that does involve Processing with a high risk in the sense of Article 35(1) GDPR, then we will carry out a data protection impact assessment and provide you with a copy of the findings free of charge. In light of the nature of our services, we have given particular attention to the innovative use or application of new technology. This is characterised by the EDPB in its guidelines as an indication that Processing might result in high risks[3]. We do not expect our Processing to result in such high risks that we need to consult the Data Protection Authority beforehand (Article 36 GDPR). You do not have the right to have a data protection impact assessment carried out for our services at your own initiative.

4.8 Security

Our information security policy provides for adequate technical, physical and organisational measures to prevent the destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data, either accidentally or unlawfully. The data protection measures take into account the state-of-the-art of the technology, the cost of implementation, the nature, scope, context, and purposes of the Processing under the agreement concluded between you and us, as well as the likelihood and severity of a violation of the personal privacy of the Data Subjects. The security level and the risks associated with the Processing and the nature of the data will be reviewed periodically, and where necessary, the security measures will be improved.

4.8.1 Access Control

Access to Personal Data is limited to authorised persons under ipnordic´s authority. These persons are bound to maintain confidentiality under the terms of a contract or a statutory obligation. The Access Rights of all employees and external parties to information and information processing facilities will be withdrawn upon the termination of the contract or agreement, and will be re-evaluated when changes occur. Access Rights of users are evaluated periodically.

4.8.2 Personnel

ipnordic runs ongoing awareness campaigns and the employees follow obligatory reoccuring security & privacy training courses during their employment.

[2] EDPB (Article 29 Working Party): Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, page 9 (https://ec.europa.eu/newsroom/document.cfm?doc_id=44137).
[3] See note 1 , page 12 – point 8.

4.8.3 Placement of Personal Data

The Personal Data processed in our role as Data Processor, in regards to the services listed in **Appendix A,** will only be stored in Approved facilities as described in **Appendix B**.

The Approved facilities can be split into two categories; Third party colocation services and Group level recipients.

The providers of third party colocation services, as described in **Appendix B,** does not access, manipulate, disseminate, store, encrypt or provide analisys of Personal Data but instead only provide electricity and housing for ipnordic owned servers, they control the purposes, condition, means and processing of Personal Data within their core network, and are therefore seen as independent Data Controllers, as described in the GDPR.

Group level recipients, are facilities that are used to store and process Personal Data in regards the delivery of services offered by ipnordic, but where the Personal Data is being processed by other entities within the Enreach Group.

By accepting this agreement, you also accept our use of the Third party colocation services and Group level recipients included in **Appendix B.**

4.8.4 Back up and disaster recovery

The purpose of a back up is to make certain that the data we Process on behalf of our Customers can be accurately and quickly recreated in the event of a security incident. Back ups are implemented on different levels in relation to the different services that we provide for our Customers. Back up´s are tested on regulary basis and annually.

ipnordic has developed documented disaster recovery plans for our services, in order to make sure that our employees know what to do in the case of a incident. These are tested and reviewed annually.

4.8.5 Encryption

When necessary, ipnordic uses encryption to protect Personal Data. For example, HTTPS with a strong TLS 1.2 protocol. When communicating with ipnordic, we will use forced TLS 1.2 on all e-mail communication going out from our core network. This is done in order to secure that Personal Data and business critical data included in the communication is kept confidential in transit. This follows Datatilsynets best practices for sending sensitive and confidential Personal Data through e-mail. This is also applicable for our Fax-2-Mail, Voicemail-2-mail and Recordings-2-mail solutions.

Most domains are set up to handle TLS 1.2 encryption and therefore we do not expect this to provide an issue in regards to e-mail communicating with our Customers. If we are sending an e-mail to a Customers domain, and the domain does not support TLS 1.2, the e-mail will bounce and it will get reported to us. We will then contact the Customer through alternative means.

4.9 Audit right

We will enable you, as a Data Processor, to demonstrate to the Data Protection Authority, a Data Subject, or some other Third Party that we perform our services in accordance with the contents of this handbook. We will do this by including compliance with the handbook in our future ISO 27001 audit. It is a goal that all entities in the Enreach Group, be ISO27001 certified. When this goal has been achieved, our compliance with this handbook will be subject to annual audits by an independent auditor. When the audit is complete, you will be able to obtain a copy of the audit certificate on request free of charge.
We will enable you, as the controller, to audit whether ipnordic is acting in accordance with this handbook. An audit can be carried out by a neutral third party auditor mutually agreed upon, and at your request. The third party auditor will be required to maintain secrecy throughout the audit and the results of the audit will be shared with you (the Data Controller) and

ipnordic. Such an audit must be announced, in writing to ipnordic, 6 weeks prior to the audit. The cost of this audit will be borne by you (the responsible person).

We will always cooperate with an audit by a regulatory authority such as the Datatilsynet, Erhvervsstyrrelsen or Forsvarsministeriet.

4.10 Erasure

In our role as Data Processor and on termination of our service to you, and in the provisioning of personal data processing services, we will be under obligation to delete all personal data processed on behalf of you and certify to you that we have done so unless Union or Member State law requires storage of the personal data.

5 Changes

We can change this handbook unilaterally. If we are planning to make a change to the handbook, then we will inform you by e-mail at least thirty (30) days before the effective date of these changes. Then we will publish a general announcement about the change on our homepage www.ipnordic.dk in our Privacy Policy.

APPENDIX A: Table of roles as Data Controller - Data Processor

Note: *in the table below we have set out the "GDPR roles" we have for the categories of Personal Data described under the heading "Data". In those cases where we think we are the Data Controller, we have described the purposes for which we will Process the relevant categories of Personal Data for.*

The "GDPR role" we fulfil depends on whether or not, and to what extent, we determine the purpose and means of the data processing[4]*. In our core network, we determine for 100% which means are used for the data processing. You make use of the systems within our core network. We have exclusive control over the configuration of these systems. According to the EDPB, that does not automatically mean we are classified as a Data Controller. It is entirely possible for a Data Processor to have exclusive control over all the means of processing*[5]*.*

Ultimately, the classification of our "GDPR role" - in the context of this handbook - is therefore determined by the answer to the question who determines the purposes of the data processing. In those cases where we Process Personal Data for our own (business) purposes, we assume that we determine the purposes of the data processing. We have initiated the Processing in question and we determine the purposes it serves. ***Example:*** *if we Process CDR (Call Detail Records), we do this so we can operate our service, so we can send you invoices, and we can establish why there is a difference of opinion in the event of a dispute, to collect information about the network traffic, and to combat fraud. For the Processing of CDRs, we are therefore a Data Controller.*

For more detailed information, see the criteria formulated by the EDPB for the classification of a provider of telecommunication services in its opinion on the concepts of Data Controller and Data Processor[6]*. On page 11 of its opinion, the EDPB states the following:*

"An interesting example of legal guidance to the private sector relates to the role of telecommunication operators: Recital 47 of Directive 95/46/EC clarifies that "where a message containing personal data is transmitted by means of a telecommunications or electronic mail service, the sole purpose of which is the transmission of such messages, the controller in respect of the personal data contained in the message will normally be considered to be the person from whom the message originates, rather than the person offering the transmission services; (...) nevertheless, those offering such services will normally be considered controllers in respect of the processing of the additional personal data necessary for the operation of the service". The provider of telecommunications services should therefore, in principle, be considered controller only for traffic and billing data, and not for any data being transmitted. This legal guidance from the Community legislator is completely in line with the functional approach followed in this opinion."

We are a Data Processor if we exclusively generate and or store the relevant Personal Data for the end customer. Examples of ipnordic as a processor, are recordings that have been stored and made available to end customers, through our online portal MinSide.

[4] See the definition of Data Controller at the beginning of this handbook. The distinction between Data Controller and Data Processor is assessed based on the opinion of the Article 29 Working Party, which is still relevant in the context of the GDPR. You can find this opinion (in English) here: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf.

[5] See note 4.

[6] See note 4.

Data ↓ / Purposes →	Role	Provision of services	Billing (Customer)	Disputes	Traffic analysis	Fraud Detection	Legal obligation	Call history
General								
Contact details Customer *Name and address details, Contact details (tel., e-mail, name) of contact persons*	Controller	●	●	●			●	
Financial details / Customer *Bank account number, CVR-number, etc.*	Controller	●	●	●			●	
ipnordic Telecommunication Solution | Communicator | Communicator PRO								
Landline communication metadata *CDR, Telephone numbers, Channel, IP Addresses, SIP, Extension, User*	Controller	●	●	●	●	●	●	●
Mobile communication metadata *CDR, Telephone numbers, IP Addresses, SIP, Extension, User, SIM number (ICCID), IMSI, MSUB, ULI*	Controller	●	●	●	●	●	●	●
User information *Name, phone number, e-mail etc..*	Controller	●	●	●				
Aggregated CDR – statistics *CDR, Names, Telephone numbers, avg. wait time, avg. call duration, avg. completed calls, avg. forwarded calls, avg. unanswered calls, etc.*	Processor							
Voicemails *Content of voicemails*	Processor							
Recordings of calls *Content of calls*	Processor							
Additional user data – Only added by end-users themselves *Position, , Meta text, City, Photo, Date of birth, Department*	Processor							

Data ↓ / Purposes →	Role	Provision of services	Billing (Customer)	Disputes	Traffic analysis	Fraud Detection	Legal obligation	Call history
SMS-Batch								
Communication metadata *CDR, Telephone numbers, Channel, IP Addresses, SIP, Extension, User*	Controller	●	●	●	●	●	●	●
Content of SMS	Processor							
Turbo-Track								
Communication metadata *CDR, IP Addresses, Extension, User, SIM number (ICCID), IMSI, MSUB, ULI*	Controller	●		●	●	●		
User information *Name, phone number, e-mail etc....*	Controller	●		●				
Location data *TrackedID, MSISDN, oordinates, longitude latitude*	Processor							
Secretary/Receptionist Service								
Communication metadata *CDR, Telephone numbers, amounts of msg sent*	Controller	●	●	●				
User information *Name, phone number, e-mail etc....*	Controller	●	●	●				
Content of message *Name of caller, Telephone number of caller, Company of caller, Short description of the nature of the call.*	Processor							

Data ↓ / Purposes →	Role	Provision of services	Billing (Customer)	Disputes	Traffic analysis	Fraud Detection	Legal obligation	Call history
WAN								
Connection details *IP address, Name and address details, Order number*	Controller	●	●		●		●	
Communication metadata *IP address (source + destination), time*	Controller				●		●	
FAX-2-MAIL / MAIL-2-FAX								
Communication metadata *CDR, Fax numbers*	Controller	●	●		●		●	
Content of communication *Faxes*	Processor							
Communicator App								
Communication metadata *CDR, sender/recipient*	Controller	●			●		●	●
SMS *Content of SMS*	Processor							
Additional user data – Only added by end-users themselves *Position, Meta text, City, Photo, Date of birth, Department*	Processor							
Calendar integration *Time, Dates, Meetings, names*	Processor							
ipnordic Meetings								
Communication metadata *UDR/CDR, sender/recipient*	Controller	●			●		●	
Content of communication *Chat / Video / Voice*	Processor							
Call recordings *Content of calls*	Processor							
Fileshare *Content of fileshare*	Processor							

APPENDIX B: List of Data Sub-Processors and Approved facilities

Sub-processers

Microsoft Ireland Operations, Ltd.
One Microsoft Place
South County Business Park
Leopardstown, Dublin 18, D18 P521,
Ireland
Hosting of mailsystem and documents.

Link Mobility A/S
Flæsketorvet 68
1711 København V
Denmark
CVR.nr. 30077520
Processsing in regards to SMS-batch

Approved facilities

Colocation services

Legal entities of colocation service providers:

TDC A/S
Teglholmsgade 1
2450 København SV
Denmark
CVR.nr. 14773908
Housing of infrastructure

GLOBALCONNECT A/S
Hørskætten 3
Klovtofte
2630 Taastrup
Denmark
CVR.nr. 26759722
Housing of infrastructure

Group level recipients

Voiceworks B.V
Verlengde Duinvalleiweg 102
Almere, 1361 BR
Netherlands
Chamber of commerce nr.: 39091093
ISO27001/ISO9001 certified
Processing in regards to ipnordic meetings

APPENDIX C: Transparency statement

In paragraph 3.2 of our Data Processing Handbook, we indicate that we make this text available to you to include in your privacy statement or otherwise make available to the Data Subjects. Because we do not receive Personal Data directly from the Data Subject, under Article 14 of the GDPR as Controller, we are obliged to communicate the information to the Data Subject as described in Article 14 (1) and (2) of the GDPR. We expect you to communicate the contents of this statement to the Data Subjects affected before you connect to our service. Below you will find the text to include in your privacy statement[1:]

Identity

Part of the public electronic communications service we provide is based on a service provided by a Group level entities. At your request, we will make the identity of the Group level recipients known to you.

Sub processers

At your request, we will provide you with a list of the sub processors that We use to provide the services to you. These suppliers process Personal Data. Data Processor Agreements are concluded with these sub processors.

Rights of the Data Subject

We allow you to exercise your rights as a data subject from Chapter 3 of the GDPR that specifically give you access to your personal data (hereinafter referred to as **"**Access Rights"). Access rights give those affected the right to do certain actions with their personal data or to limit the processing of that personal data.

Because we and/or our Group level recipients process Personal Data of stakeholders, we can at your request modify, delete or export personal data to a subsequent provider. You can exercise your rights by contacting compliance@ipnordic.dk