

# Notisum's general terms and conditions for network services

Valid from 2023-12-01, until further notice.

## 1. General

---

1.1. These general terms and conditions apply to the internet services, consulting products and similar services and products provided at any given time by Notisum AB, corporate registration no. 556516-2467 ("**Notisum**").

1.2. Notisum continuously updates its range of services and products and reserves the right to amend, delete or add information in the services and products offered and to cease providing them.

1.3. Agreements on access to services and products provided by Notisum are entered into by a company or other legal entity (the "**Licensee**") for use of the services and products by its employees [and contractors] (the "**Users**"). All Users must accept these general terms and conditions when first logging into the Services (defined below).

1.4. A subscription agreement between Notisum and the Licensee (the "**Subscription Agreement**") covers the services and products included in the Subscription Agreement (the "**Services**") at any given time and they are provided on the financial terms agreed by the parties in the Subscription Agreement and in accordance with these general terms and conditions.

1.5. The Licensee may not grant the use of or transfer its rights under the Subscription Agreement to a third party without Notisum's written permission given in advance. In the event of a transfer, a new party to the Agreement must confirm in writing that it accepts the provisions of the Subscription Agreement and these general terms and conditions.

## 2. Grant of use and rights

---

2.1. All rights to the Services and their contents, including copyright and all other intellectual property rights, are the property of Notisum and/or third parties with which Notisum has entered into agreements. Information on copyright and other notices regarding right of ownership contained in the Services or on a supplied product and in documentation relating thereto must be retained by the Licensee and may not be removed or rendered illegible.

2.2. The Licensee and the Users receive no right to the Services over and above what is expressly set out in the Subscription Agreement and in these general terms and conditions.

2.3. Notisum grants the Licensee a non-exclusive, non-assignable and non-transferable right to allow the Users to use the Services during the term of the Subscription Agreement in accordance with the Subscription Agreement and these general terms and conditions and, in connection therewith, to copy, process or produce summaries of the contents of the Services such as lists of laws and other similar work products that are wholly or partly based on the Services ("**Results**"), all for the Licensee's internal use and in accordance with the Subscription Agreement and these general terms and conditions.

2.4. "**The Licensee's internal use**" means use of the Services and the Results for the Licensee's own activities, but not that the Licensee grants the use of the Services or makes them available to a third party. Further details regarding the boundaries between permitted and prohibited use of the Services and the Results are set out below.

### 3. More details regarding use of the Services

---

3.1. The Services may only be used by the Users for the purpose for which they have been produced and only for lawful purposes. The Users may not grant the use of or transfer their right to use the Services or parts thereof or otherwise dispose of the Services. If a User ceases to be an employee or contractor of the Licensee, its right to use the Services in connection therewith ceases.

3.2. The Users are responsible for storing passwords or other user authorisations in a secure manner. The Users can ask Notisum to block the Services or to provide the User with a new password.

3.3. The Users may not transfer, grant the use of or otherwise disseminate passwords or other user authorisations allotted to them by Notisum over and above what is required for the Users' own use of the Service.

3.5. When using the Services, the Users are also required to comply with the other regulations, instructions and restrictions applying to each Service and the other instructions issued by Notisum or a third party with which Notisum has entered into an agreement.

3.6. Notisum is entitled to suspend a User from further use of the Services without prior warning if the User is suspected of using the Services in breach of these general terms and conditions.

3.7. The Users may store Results and documents uploaded by the User with Notisum within the framework of the Services and subject to the more detailed restrictions issued by Notisum. The Licensee is responsible for ensuring that all such storage and processing of the material takes place in accordance with legislation in force at any given time. Notisum must keep such material confidential. The Licensee must indemnify Notisum for all claims for compensation, costs and any other damages that such material may cause Notisum. Notisum reserves the right to delete such material if it is suspected that it has not been stored and/or processed in accordance with applicable legislation and if the Users' right to use the Services ceases. The User is responsible for backing up the Results and documents uploaded by the User.

### 4. Trial period

---

4.1. If Notisum and the Licensee have entered into a specific agreement on a trial period for the Services, the following applies.

4.2. Agreed and named Users may have access to the Services for the limited period specified in the agreement (the "**Trial Period**") for the purpose of trying them out. No amount is payable to Notisum for such use of the Services.

4.3. These general terms and conditions apply *mutatis mutandis* to all use of the Services during the Trial Period, except for the payment provision, paragraph 9.

## 5. Processing of personal data

---

5.1. Notisum is the data controller for the personal data provided by the Licensee and/or the Users when ordering and/or using the Services. More detailed information on how Notisum processes personal data is provided in [Notisum's privacy policy](#)

5.2. In accordance with the General Data Protection Regulation, Notisum will have a role as a data processor in relation to the Licensee, as the data controller, in the event that Notisum and the Licensee have agreed that personal data may be stored in the Services. In such cases, Annex 1, Data Processing Agreement, applies if Notisum processes personal data on behalf of the Licensee.

## 6. Technical requirements

---

6.1. See the Notisum website [www.notisum.se] for technical requirements applicable at any given time that must be met in order for the Users to access the Services and the proper functioning of the Services.

6.2. The Licensee and the User are liable for compliance with the technical requirements and the existence of a working connection between the User and the Connection Point (see the definition below). Furthermore, the Licensee and the User are liable for the associated costs and for installation of any required software.

## 7. Delivery and support

---

7.1. The Services are provided at the connection point designated by Notisum (the “**Connection Point**”). Unless otherwise agreed by the parties, the Connection Point is the point or points where Notisum connects the Services and the internet.

7.2. See the Notisum website [www.notisum.se] for the opening hours etc. of the Service. During the term of the Agreement, Notisum is entitled to close down one or more Services in full or in part in order to carry out updates, maintenance and similar operations (see the Notisum website [www.notisum.se] for more detailed information on scheduled maintenance operations).

7.3. Technical support and user support, (collectively referred to as “**Support**”) for the Services is provided by Notisum or by a third party on behalf of Notisum on weekdays and during office hours (see the Notisum website [www.notisum.se] for the contact details and opening hours etc. of the local support). Until Notisum states otherwise, Support is provided without any specific payment.

7.4. Support does not include support, maintenance, troubleshooting remedying of faults or similar actions regarding the Licensees' or the Users' software or hardware, internet connections and/or products/services that have not been provided by Notisum or for which Notisum is not expressly responsible. Nor does Support include questions regarding the application of the legislation and other regulations involved in the delivery of the Services.

## 8. Faults or defects

---

8.1. In the event of a fault or defect in the Services at the Connection Point, the Licensee must contact Notisum for action to be taken (see the Notisum website [www.notisum.se] for contact details for fault reporting).

8.2. Notisum is responsible for faults or defects in the Services that mean that the contents or functioning of the Services substantially fail to comply with Notisum's service descriptions applied at any given time and that the fault or defect is attributable to Notisum. Notisum is not liable for faults or defects attributable to the Licensee, the Users or third parties for which Notisum is not expressly liable.

8.3. Since the Services are dependent on the internet, the Licensee acknowledges that interruptions, delays, bugs and similar obstacles between the Services and the Users, such as on the internet, do not constitute a fault in the Services.

8.4. In the event of a fault or defect in the Services that is not remedied within a reasonable time and that means that the Users' use of the Services is adversely affected to a substantial extent, the Licensee is entitled to receive a reasonable price reduction from when the fault is reported until the fault or defect has been corrected. If the fault or defect is substantial and is not corrected within a reasonable deadline, the Licensee is entitled to terminate all or the relevant parts of the Subscription Agreement. This, together with the provisions of paragraph 11, comprehensively governs Notisum's liability in the event of a fault or defect in the Services.

## 9. Payment

---

9.1. The Licensee is obliged to pay fees agreed or otherwise applicable at any given time for all use of the Services.

9.2. Notisum is entitled to increase the fee with immediate effect if the increase is directly attributable to external factors such as changes in exchange rates, tax or similar general duties and in other similar circumstances of economic significance for the Service beyond Notisum's control and which affect the cost of providing the Service. Unless otherwise is stated in these general terms and conditions Notisum must give notice of changes in fees that are not attributable to external factors no later than thirty (30) days before the changes in fees enter into force, whereupon the Licensee has the option of terminating the Subscription Agreement by giving thirty (30) days' notice.

9.3. The fee for a subscription is paid in advance against an invoice subject to payment terms of thirty (30) days net from the invoice date. Any special fees for connection to and use of certain types of Services are paid in arrears against an invoice, subject to the aforesaid payment terms.

9.4. In the event of a delay, statutory interest on overdue payment is charged from the due date. A reminder fee will be charged if a payment reminder is issued. In the event of a delay in payment, Notisum is entitled to temporarily suspend a User's access to the Services until all amounts due have been paid and/or give notice of termination of the Subscription Agreement with effect fourteen (14) days after a payment reminder.

9.5. All amounts in the Subscription Agreement and Notisum's price list exclude VAT. The Customer is responsible for payment of VAT, other taxes and public charges payable or that may be payable in respect of the Services.

9.6. In the event of termination, no fixed fees already paid are refunded except in the event of termination in accordance with paragraphs 8.4, 14.3 and 16. Upon termination, the Customer is obliged to pay Notisum any special expenses invoiced in arrears in accordance with paragraph 9.3.

## 10. Force majeure

---

10.1. Neither Party is liable vis-à-vis the other Party for the fulfilment of obligations under the Subscription Agreement or these general terms and conditions when such is prevented by circumstances beyond the control of a party or its suppliers ("**Force Majeure**"), including but not limited to war and mobilisation, natural disasters, epidemics, lockouts or other labour conflicts, lack of natural resources, fire, damage to equipment used, amended public authority regulations, intervention by a public authority, interruption of public transport including, inter alia, energy supply and computer viruses in the Services as well as import and export prohibitions and other prohibitions beyond a Party's control.

10.2. The Party wishing to cite Force Majeure is required to notify the other Party in writing without delay when such a circumstance arises and when it ceases.

10.3. If the performance and fulfilment of these general terms and conditions for the Subscription Agreement are rendered impossible for ninety (90) days due to Force Majeure, either Party is entitled to cancel the Subscription Agreement by giving notice in writing to the other Party.

## **11. Limitation of liability and claims**

---

11.1. The Licensee must compensate Notisum for any damages sustained by Notisum as a result of use of the Services by the Licensee and/or a User in breach of the Subscription Agreement and these general terms and conditions or in any way that causes damage to Notisum.

11.2. Except as set out above in paragraph 8, Notisum is not liable for the functioning or quality of the Services. Notisum is not liable for factual errors in the Services or for any damages that may arise as a result thereof. Nor will Notisum be liable for any advice or information that the Licensee or a User has been given the opportunity to obtain from a consultant employed by Notisum or a third party in connection with the Services.

11.3. Notisum is not liable for loss of production, loss of profits, loss of income, consequential damages or other indirect damages or loss.

11.4. Notisum's total liability vis-à-vis the Licensee, except in cases of gross negligence or intent, is limited to the payment received by Notisum from the Licensee in accordance with the Subscription Agreement during the preceding twelve (12) months. Notisum is not liable vis-à-vis anyone other than the Licensee such as the Users, the Licensee's customers, suppliers or partners or any authority overseeing the Licensee.

11.5. Complaints and other claims must be filed in writing without undue delay from when a Party discovered or should have discovered the circumstance giving rise to the claim, though no later than within six (6) months from the occurrence of the circumstance, after which the claim otherwise expires.

## **12. Customer data**

---

12.1. Notisum it is not entitled to make use of any data that the Licensee, either itself or through a User, submits to Notisum or that Notisum otherwise obtains access to through the Licensee's use of the Services ("**Customer Data**"), unless otherwise specified in this Agreement.

12.2. Notisum may use Customer Data to carry out the assignment, for statistical purposes and to improve and develop Notisum's Services.

12.3. Notisum may also transfer Customer Data to group companies and suppliers if necessary to enable it to deliver or develop the Services.

12.4. The Licensee must ensure that Customer data is free from viruses, trojans, worms or other software or code that could damage the Services or Notisum's IT environment.

## **13. Intellectual property rights**

---

13.1. These general terms and conditions do not mean that copyright or other intellectual property rights to the Services is transferred to the Licensee, a User or other third party. The Licensee and the User may not copy, modify or otherwise process software or other materials associated with the Services or transfer or grant the use of the right to such software or materials to another party unless such is provided in these general terms and conditions or has otherwise been agreed in writing with Notisum.

13.2. The Licensee undertakes to defend Notisum at its own expense if a claim is filed or an action is brought against Notisum for infringement due to use of the Services by the Licensee or User in breach

of these general terms and conditions. The Licensee undertakes to compensate Notisum for all costs and damages that Notisum may be required to pay due to a settlement or judgment.

## 14. Term of the Agreement

---

14.1. The Subscription Agreement applies, unless otherwise agreed, from when the Agreement is signed and thereafter for twelve (12) months.

14.2. If the Subscription Agreement has not been terminated no later than sixty (60) days prior to the end of the term of the Agreement by means of notice of termination given by the Licensee to Notisum no later than that date, the Subscription Agreement is automatically extended by twelve (12) months or by the agreed extension period, with the corresponding notice period. In the event of an extension of the Subscription Agreement, Notisum's general terms and conditions and prices in force at any given time apply. The notice of termination must be given in writing.

14.3. In addition to what is otherwise specified in the Subscription Agreement and these general terms and conditions, a party is entitled to terminate the Subscription Agreement with immediate effect if the other party (a) is in breach of the Agreement and fails to adopt a remedy within twenty (20) days of receipt of a written reminder of the breach of the agreement from the other party, or (b) initiates a liquidation procedure, applies for bankruptcy or is declared bankrupt, suspends payments or may otherwise be feared to be on the way towards insolvency.

14.4. The Licensee no longer has any right to use the Services as of the date when the Subscription Agreement ceases. If Notisum has stored Results from the Users or other materials in connection with the Services, Notisum is entitled to delete such material ninety (90) days after the Subscription Agreement ceases.

## 15. Confidentiality

---

15.1. "**Confidential Information**" means any information of an economic, technical, commercial or other nature relating to the parties and their affiliated companies, whether or not the information has been documented in writing. Nevertheless, information that is public knowledge or that has become public knowledge other than through breach of these general terms and conditions by the party receiving it must not be regarded as Confidential Information.

15.2. The parties undertake not to disclose, in whole or in part, Confidential Information received in connection with the Subscription Agreement and these general terms and conditions relating to the other party or to a third party unless the other party has given its prior written consent thereto or the party disclosing the Confidential Information has an obligation to do so in accordance with an applicable law, an enforceable judgment, a binding decision by a public authority or directives or applicable regulations for regulated markets. The parties may not make use of Confidential Information for any purpose other than to exercise their rights and obligations in accordance with the Subscription Agreement and these general terms and conditions. A party must adopt all necessary measures to prevent prohibited dissemination or use of Confidential Information by its employees or contractors.

15.3. The parties' confidentiality obligations must apply without limitation in time.

15.4. Notisum may, by special agreement with the Licensee, indicate for marketing purposes that the Licensee is a user of the Services.

## **16. Amendment of general terms and conditions**

---

Notisum is entitled to amend these general terms and conditions without prior approval from the Licensee. The Licensee will be informed if such amendments are substantially detrimental to it and the amendments enter into force thirty (30) days after the Licensee was notified of the amendment. In the event of any amendment that is substantially detrimental to the Licensee, the Licensee is entitled to notify Notisum, no later than fourteen (14) days before the amendment enters into force, that the Licensee gives notice of termination of the Subscription Agreement from the date of entry into force of the amendment. The notice of termination must be given in writing.

## **17. Notices**

---

17.1. Notisum issues notices to the Licensee via the Services, by means of a letter to the address communicated by the Licensee, by email to the email address communicated by the Licensee or as otherwise agreed by the parties.

17.2. Notices to the Licensee regarding amendments to the terms and conditions and any other notices under these general terms and conditions must be considered to have been received by the Licensee no later than three (3) days after the notice was sent by post to the latest address of which Notisum was notified in writing by the Licensee. Notices issued in the Service or that are sent by email to the latest email address of which Notisum was notified by the Licensee will be considered to have been received by the Licensee immediately.

17.3. The Licensee is required to notify Notisum in the Service of updates to its address, email address or other contact details provided to Notisum.

17.4. The Licensee may issue notices to Notisum regarding these general terms and conditions by using Notisum's user support in the Services.

## **18. Choice of law and jurisdiction**

---

Swedish substantive law will apply to these general terms and conditions. Disputes relating to these general terms and conditions will be heard by the Stockholm District Court as the court of first instance.

# Annex 1 Data Processing Agreement

---

This Data Processing Agreement is between the Licensee, Data Controller, and Notisum, Data Processor, each a "Party" and collectively the "Parties".

The parties HAVE AGREED on the following Standard Contractual Clauses (the Clauses) in order to meet the requirements of the GDPR and to ensure the protection of the rights of the data subject.

## 1 Preamble

- 1.1 These Contractual Clauses (the Clauses) set out the rights and obligations of the data controller and the data processor, when processing personal data on behalf of the data controller.
- 1.2 The Clauses have been designed to ensure the parties' compliance with Article 28(3) of Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).
- 1.3 In the context of the provision of using Notisum's internet services, the data processor will process personal data on behalf of the data controller in accordance with the Clauses. The Clauses shall take priority over any similar provisions contained in other agreements between the parties.
- 1.4 Four appendices are attached to the Clauses and form an integral part of the Clauses.
- 1.5 Appendix A contains details about the processing of personal data, including the purpose and nature of the processing, type of personal data, categories of data subject and duration of the processing.
- 1.6 Appendix B contains the data controller's conditions for the data processor's use of sub-processors and a list of sub-processors authorised by the data controller.
- 1.7 Appendix C contains the data controller's instructions with regards to the processing of personal data, the minimum-security measures to be implemented by the data processor and how audits of the data processor and any sub-processors are to be performed.
- 1.8 Appendix D contains provisions for other activities which are not covered by the Clauses.
- 1.9 The Clauses along with appendices shall be retained in writing, including electronically, by both parties.
- 1.10 The Clauses shall not exempt the data processor from obligations to which the data processor is subject pursuant to the General Data Protection Regulation (the GDPR) or other legislation.



## **2 The rights and obligations of the data controller**

- 2.1 The data controller is responsible for ensuring that the processing of personal data takes place in compliance with the GDPR (see Article 24 GDPR), the applicable EU or Member State data protection provisions and the Clauses.
- 2.2 The data controller has the right and obligation to make decisions about the purposes and means of the processing of personal data.
- 2.3 The data controller shall be responsible, among other, for ensuring that the processing of personal data, which the data processor is instructed to perform, has a legal basis.

## **3 The data processor acts according to instructions.**

- 3.1 The data processor shall process personal data only on documented instructions from the data controller, unless required to do so by Union or Member State law to which the processor is subject. Such instructions shall be specified in appendices A and C. Subsequent instructions can also be given by the data controller throughout the duration of the processing of personal data, but such instructions shall always be documented and kept in writing, including electronically, in connection with the Clauses.
- 3.2 The data processor shall immediately inform the data controller if instructions given by the data controller, in the opinion of the data processor, contravene the GDPR or the applicable EU or Member State data protection provisions.

## **4 Confidentiality**

- 4.1 The data processor shall only grant access to the personal data being processed on behalf of the data controller to persons under the data processor's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need-to-know basis. The list of persons to whom access has been granted shall be kept under periodic review. On the basis of this review, such access to personal data can be withdrawn, if access is no longer necessary, and personal data shall consequently not be accessible anymore to those persons.
- 4.2 The data processor shall at the request of the data controller demonstrate that the concerned persons under the data processor's authority are subject to the abovementioned confidentiality.

## 5 Security of processing

- 5.1 Article 32 GDPR stipulates that, taking into account the state of the art, the costs of implementation and the nature, scope, context, and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the data controller and data processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.
- 5.2 The data controller shall evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. Depending on their relevance, the measures may include the following:
  - 5.3 Pseudonymisation and encryption of personal data.
  - 5.4 The ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services.
  - 5.5 The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.
  - 5.6 A process for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
- 5.7 According to Article 32 GDPR, the data processor shall also – independently from the data controller – evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. To this effect, the data controller shall provide the data processor with all information necessary to identify and evaluate such risks.
- 5.8 Furthermore, the data processor shall assist the data controller in ensuring compliance with the data controller's obligations pursuant to Articles 32 GDPR, by inter alia providing the data controller with information concerning the technical and organisational measures already implemented by the data processor pursuant to Article 32 GDPR along with all other information necessary for the data controller to comply with the data controller's obligation under Article 32 GDPR.
- 5.9 If subsequently – in the assessment of the data controller – mitigation of the identified risks requires further measures to be implemented by the data processor, than those already implemented by the data processor pursuant to Article 32 GDPR, the data controller shall specify these additional measures to be implemented in Appendix C.

## **6 Use of sub-processors**

- 6.1 The data processor shall meet the requirements specified in Article 28(2) and (4) GDPR in order to engage another processor (a sub-processor).
- 6.2 The data processor shall therefore not engage another processor (sub-processor) for the fulfilment of the Clauses without the prior general written authorisation of the data controller.
- 6.3 The data processor has the data controller's general authorisation for the engagement of sub-processors. The data processor shall inform in writing the data controller of any intended changes concerning the addition or replacement of sub-processors at least 3 months in advance, thereby giving the data controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). Longer time periods of prior notice for specific sub-processing services can be provided in Appendix B. The list of sub-processors already authorised by the data controller can be found in Appendix B.
- 6.4 Where the data processor engages a sub-processor for carrying out specific processing activities on behalf of the data controller, the same data protection obligations as set out in the Clauses shall be imposed on that sub-processor by way of a contract or other legal act under EU or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the Clauses and the GDPR.
- 6.5 The data processor shall therefore be responsible for requiring that the sub-processor at least complies with the obligations to which the data processor is subject pursuant to the Clauses and the GDPR.
- 6.6 A copy of such a sub-processor agreement and subsequent amendments shall – at the data controller's request – be submitted to the data controller, thereby giving the data controller the opportunity to ensure that the same data protection obligations as set out in the Clauses are imposed on the sub-processor. Clauses on business related issues that do not affect the legal data protection content of the sub-processor agreement, shall not require submission to the data controller.
- 6.7 If the sub-processor does not fulfil his data protection obligations, the data processor shall remain fully liable to the data controller as regards the fulfilment of the obligations of the sub-processor. This does not affect the rights of the data subjects under the GDPR – in particular those foreseen in Articles 79 and 82 GDPR – against the data controller and the data processor, including the sub-processor.

## **7 Transfer of data to third countries or international organisations**

- 7.1 Any transfer of personal data to third countries or international organisations by the data processor shall only occur on the basis of documented instructions from the data controller and shall always take place in compliance with Chapter V GDPR.
- 7.2 In case transfers to third countries or international organisations, which the data processor has not been instructed to perform by the data controller, is required under EU or Member State law to which the data processor is subject, the data processor shall inform the data controller of that legal requirement prior to processing unless that law prohibits such information on important grounds of public interest.
- 7.3 Without documented instructions from the data controller, the data processor therefore cannot within the framework of the Clauses:
- 7.4 Transfer personal data to a data controller or a data processor in a third country or in an international organization.
- 7.5 Transfer the processing of personal data to a sub-processor in a third country.
- 7.6 Have the personal data processed in by the data processor in a third country
- 7.7 The data controller's instructions regarding the transfer of personal data to a third country including, if applicable, the transfer tool under Chapter V GDPR on which they are based, shall be set out in Appendix C.6.
- 7.8 The Clauses shall not be confused with standard data protection clauses within the meaning of Article 46(2)(c) and (d) GDPR, and the Clauses cannot be relied upon by the parties as a transfer tool under Chapter V GDPR.

## 8 Assistance to the data controller

- 8.1 Taking into account the nature of the processing, the data processor shall assist the data controller by appropriate technical and organisational measures, insofar as this is possible, in the fulfilment of the data controller's obligations to respond to requests for exercising the data subject's rights laid down in Chapter III GDPR.

This entails that the data processor shall, insofar as this is possible, assist the data controller in the data controller's compliance with:

- a The right to be informed when collecting personal data from the data subject.
- b The right to be informed when personal data have not been obtained from the data subject.
- c The right of access by the data subject
- d The right to rectification
- e The right to erasure ('the right to be forgotten')
- f The right to restriction of processing
- g Notification obligation regarding rectification or erasure of personal data or restriction of processing
- h The right to data portability
- i The right to object
- j The right not to be subject to a decision based solely on automated processing, including profiling.

- 8.2 In addition to the data processor's obligation to assist the data controller pursuant to Clause 5.3., the data processor shall furthermore, taking into account the nature of the processing and the information available to the data processor, assist the data controller in ensuring compliance with:

- a The data controller's obligation to without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority, The Swedish Data Protection Agency, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;
- b The data controller's obligation to without undue delay communicate the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.
- c The data controller's obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a data protection impact assessment).
- d The data controller's obligation to consult the competent supervisory authority, the Swedish Data Protection Agency, prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the data controller to mitigate the risk.

- 8.3 The parties shall define in Appendix C the appropriate technical and organisational measures by which the data processor is required to assist the data controller as well as the scope and the extent of the assistance required. This applies to the obligations foreseen in Clause 8.1. and 8.2.

## **9 Notification of personal data breach**

- 9.1 In case of any personal data breach, the data processor shall, without undue delay after having become aware of it, notify the data controller of the personal data breach.
- 9.2 The data processor's notification to the data controller shall, if possible, take place within 36 hours after the data processor has become aware of the personal data breach to enable the data controller to comply with the data controller's obligation to notify the personal data breach to the competent supervisory authority, cf. Article 33 GDPR.
- 9.3 In accordance with Clause 9(2)(a), the data processor shall assist the data controller in notifying the personal data breach to the competent supervisory authority, meaning that the data processor is required to assist in obtaining the information listed below which, pursuant to Article 33(3) GDPR, shall be stated in the data controller's notification to the competent supervisory authority:
- a. The nature of the personal data including where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned.
  - b. The likely consequences of the personal data breach.
  - c. The measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
- 9.4 The parties shall define in Appendix C all the elements to be provided by the data processor when assisting the data controller in the notification of a personal data breach to the competent supervisory authority.

## **10 Erasure and return of data.**

- 10.1 On termination of the provision of personal data processing services, the data processor shall be under obligation to delete all personal data processed on behalf of the data controller and certify to the data controller that it has done so unless Union or Member State law requires storage of the personal data.

## **11 Audit and inspection**

- 11.1 The data processor shall make available to the data controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and the Clauses and allow for and contribute to audits, including inspections, conducted by the data controller or another auditor mandated by the data controller.
- 11.2 Procedures applicable to the data controller's audits, including inspections, of the data processor and sub-processors are specified in appendices C.7. and C.8.

- 11.3 The data processor shall be required to provide the supervisory authorities, which pursuant to applicable legislation have access to the data controller's and data processor's facilities, or representatives acting on behalf of such supervisory authorities, with access to the data processor's physical facilities on presentation of appropriate identification.

## **12 The parties' agreement on other terms**

- 12.1 The parties may agree other clauses concerning the provision of the personal data processing service specifying e.g., liability, if they do not contradict directly or indirectly the Clauses or prejudice the fundamental rights or freedoms of the data subject and the protection afforded by the GDPR.

## **13 Commencement and termination**

- 13.1 The Clauses is an integrated part of the general terms of conditions and is valid from the acceptance of those.
- 13.2 Both parties shall be entitled to require the Clauses renegotiated if changes to the law or inexpediency of the Clauses should give rise to such renegotiation.
- 13.3 The Clauses shall apply for the duration of the provision of personal data processing services. For the duration of the provision of personal data processing services, the Clauses cannot be terminated unless other Clauses governing the provision of personal data processing services have been agreed between the parties.
- 13.4 If the provision of personal data processing services is terminated, and the personal data is deleted or returned to the data controller pursuant to Clause 10.1. and Appendix C.4., the Clauses may be terminated by written notice by either party.

# **Appendix A - Information about the processing**

## **A.1. The purpose of the data processor's processing of personal data on behalf of the data controller is:**

The Data Processor is delivering internet services to the Data Controller to support regulatory monitoring and handling legal compliance matters.

## **A.2. The data processor's processing of personal data on behalf of the data controller shall mainly pertain to (the nature of the processing):**

Notisum's internet services may be used to collect, process, and store personal information as part of the data controllers work with legal compliance matters. The Data Processor will only process personal data according to the Instruction from the Data Controller.

## **A.3. The processing includes the following types of personal data about data subjects:**

The categories of personal data that are processed constitute all types of information that could potentially be relevant for handling compliance matters, e.g., personal data in connection with:

- a. identifying responsible natural persons for legal monitoring, auditing and other processes assisted by Notisum's internet services,
- b. storage of compliance audit proof documents and photos, permits and other internal documents,
- c. other information that appears from the content of data material that can be used in the process of regulatory monitoring and legal compliance audits.

The abovementioned list is a non-exhaustive list, and the data controller has the overall responsibility to ensure, that they have the right to process the personal data, which is uploaded to Notisum's internet services. The data processor does not control the types of documents and their content.

## **A.4. Processing includes the following categories of data subject:**

The data subjects to whom the personal data relate will be parties who have or have had a relationship with the Data Controller and whose information is relevant to process by the Data Controller when conducting its process of regulatory monitoring and legal compliance audits, including among others.

- a. management, employees, and advisors,
- b. parties who assist the Data Controller with tasks within the area of regulatory monitoring and legal compliance audits from a practical, technical, economic, or legal perspective,
- c. parties whose information may prove relevant in connection with the conduct of compliance audits, or
- d. information about parties who send or receive e-mails from the Data Controller, or whose information appears inside such e-mails, if such emails are store in Notisum's web services.

The abovementioned list is a non-exhaustive list, and the data controller has the overall responsibility to ensure, that they have the right to process the personal data, which is uploaded to Notisum's internet services. The data processor does not control the types of documents and their content.



**A.5. The data processor's processing of personal data on behalf of the data controller may be performed when the Clauses commence. Processing has the following duration:**

The processing is not time-limited and lasts until the Clauses are terminated or terminated by one of the Parties.

## Appendix B - Authorized sub-processors

### B.1. Approved sub-processors.

On commencement of the Clauses, the data controller authorises the engagement of the following sub-processors:

NAME	ORG NO:	ADDRESS	DESCRIPTION OF PROCESSING
Karnov Group Denmark A/S	10361990	Sankt Petri Passage 5, St. 1165 Copenhagen	E-mail handling and data storage.  Karnov Group Denmark uses Microsoft Azure as cloud computing platform and data is stored on servers inside the EU (Microsoft West Europe (Netherlands) Microsoft North Europe (Ireland)).
Notisum Aps	36020156	Sankt Petri Passage 5, St. 1165 Copenhagen	Using the Notisum platform and content in Denmark
Echoline SAS	517886990	5, esplanade Compans Caffarelli – CS 57130 – Bâtiment A - 31071 TOULOUSE Cédex 7. FRANCE	Using the Notisum platform and content in France
DL Moberg AB	559132-7324	Vattenverksvägen 8, 184 33 ÅKERSBERGA	Database development and maintenance, customer support and customer implementation projects.
Mandoit AB	556063-8644	Sköldvägen 17. 187 36 TÄBY	Database development and maintenance, customer support and customer implementation projects.
Kopparklinten AB	556703-5612	Vindarnas väg 8, 42935 KULLAVIK	Database development and maintenance, customer support and customer implementation projects.

The data controller shall on the commencement of the Clauses authorise the use of the abovementioned sub-processors for the processing described for that party. The data processor shall not be entitled – without the data controller’s explicit written authorisation – to engage a sub-processor for a ‘different’ processing than the one which has been agreed upon or have another sub-processor perform the described processing.

## **B.2. Prior notice for the authorisation of sub-processors**

The data processor's request for authorisation of a different sub-processor or change of processing activities must be received by the data controller at least 3 months prior to the application or change will commence. The data controller may only refuse approval if the data controller has reasonable, specific reasons for this.

# **Appendix C - Instruction pertaining to the use of personal data.**

## **C.1. The subject of/instruction for the processing**

The data processor's processing of personal data on behalf of the data controller shall be carried out by the data processor performing the following:

The data processor delivers Notisum's internet services, where personal information is collected, processed, and stored. The data processor may only process such personal data to the extent necessary to perform the tasks described in this appendix and the instructions documented by the data controller at any time.

The data processor is delivering the Notisum's internet services to the data controller to support the data controller's regulatory monitoring and handling of legal compliance matters.

## **C.2. Security of processing**

The level of security shall take into account:

The nature, scope context and purposes of the processing activity as well as the risk for the rights and freedoms of natural persons, the data processor shall maintain an appropriate level of data security in accordance with best practice.

The Data Processor implements the following measures, which have been agreed with the Data Controller:

- a. At all times comply with the provisions described in the General Data Protection Regulation.
- b. Ensure the necessary technical and organizational measures against information being accidentally or illegally destroyed, lost, or impaired and that it comes to the knowledge of unauthorized persons, misused, or otherwise processed in violation of the General Data Protection Regulation.
- c. Protection of data where it is transmitted and stored. Data is encrypted in the transfer between the data controller and the data processor.
- d. Access to personal data is ensured only to relevant users.
- e. The ability to ensure the ongoing confidentiality, integrity, availability and robustness of processing systems and services.
- f. Using logging
- g. Remote security of premises where personal data is processed.
- h. Perform annual risk assessments to determine if the agreed measures are sufficient.

## **C.3. Assistance to the data controller**

The data processor shall insofar as this is possible – within the scope and the extent of the assistance specified below – assist the data controller in accordance with Clause 8.1. and 8.2. by implementing the following technical and organisational measures:

The data processor shall assess the need for, and to the extent necessary implement, processes that ensure assistance to the data controller in fulfilling its obligations to respond to requests for the exercise of the data subject's rights.

The data processor must assess the need for, and to the extent necessary implement, processes that ensure assistance to the data controller, with all the information available to the data processor that is needed for the data controller to assess the extent of the breach, report the breach to the supervisory authority and notify the data subjects.

In the event of a breach of personal data security, the following information must be submitted to the Data Controller:

<b>Date and time:</b>	The breach of personal data was detected on [date], at [time].
<b>Circumstances of data breach:</b>	The breach is due to [the circumstances of the breach of data security].
<b>The character / nature of the breach:</b>	At present, it is noted that [Insert information about the nature of the breach. As long as it is possible to determine the following: 1) Categories and the approximate number of data subjects involved 2) Categories and the approximate amount of personal data information involved.]
<b>Other relevant information</b>	At this point, it is noted that [Indicate other information about the breach of personal data that may be useful to the data controller's assessment of the impact of the breach].
<b>Actions taken:</b>	In order to limit the extent and consequences of the breach, we have so far [Measures taken by Notisum to address the breach of personal data, including measures taken to limit any harmful effects].
<b>Point of Contact at the data processor:</b>	[Contact information].

The information must be sent to the data controller's contact person as specified in clause 14 of the Clauses.

The data controller has the right at any time to request that answers be specified in the event of any questions of doubt.

#### **C.4. Storage period/erasure procedures**

Personal data is stored for up to 12 months after termination of the agreement after which the personal data is automatically erased by the data processor.

Upon termination of the provision of personal data processing services, the data processor shall delete the personal data in accordance with Clause 10.1., unless the data controller – after the signature of the contract – has modified the data controller's original choice. Such modification shall be documented and kept in writing, including electronically, in connection with the Clauses.

#### **C.5. Processing location**

Processing of the personal data under the Clauses cannot be performed at other locations than the following without the data controller's prior written authorisation:

Notisum's internet services are hosted in Microsoft azure and are therefore located on Microsoft servers within the EU. Data is located at the datacentre Microsoft EU West in the Netherlands and some of the data is replicated at the datacentre Microsoft EU North in Ireland.

Microsoft Azure uses sub-processors the list can be found at [https://aka.ms/Online\\_Serv\\_Subcontractor\\_List](https://aka.ms/Online_Serv_Subcontractor_List), who provides technologies to power or provide ancillary services to certain Microsoft Online Services, or who provides contract staff.

## C.6. Instruction on the transfer of personal data to third countries

If the data controller does not in the Clauses or subsequently provide documented instructions pertaining to the transfer of personal data to a third country, the data processor shall not be entitled within the framework of the Clauses to perform such transfer.

NAME	ADDRESS	DESCRIPTION OF PROCESSING	LEGAL BASIS FOR THE PROCESSING
Karnov Group Denmark	Microsoft West Europe (Netherlands) and Microsoft North Europe (Ireland)	E-mail handling and data storage. Karnov Group Denmark uses Microsoft Azure as a sub-processor. Data is stored on servers inside the EU and will generally <b>not</b> be transferred outside of the EU.	Standard Contractual Clauses (SCC) and supplementary measures.

## C.7. Procedures for the data controller's audits, including inspections, of the processing of personal data being performed by the data processor.

The data processor shall, at the request of the data controller, submit a management statement declaring the data processor's compliance with the data protection regulation, data protection provisions of other EU or national law and these Clauses.

The data controller may request additional information in the form of a written inspection with a questionnaire or using another method.

In addition, the data controller or a representative of the data controller has access to carry out inspections, including physical inspections, on the premises from which the data processor performs the processing of personal data, including physical premises and systems used for or in connection with the processing. Such inspections may be carried out when the data controller deems it necessary.

In addition to the planned inspection, the data controller may carry out an inspection at the data processor when the data controller deems it necessary e.g., in connection with handling breaches of personal data. Inspection visits can be made by relevant employees.

In addition, the data controller or a representative of the data controller has access to carry out inspections, including physical inspections, on the premises from which the data processor performs the processing of personal data, including physical premises and systems used for or in connection with the processing. Such inspections may be carried out when the data controller deems it necessary, but not without prior notification to the data processor.

In addition to the planned inspection, the data controller may carry out an inspection at the data processor, when the data controller deems it necessary, e.g., in connection with handling breaches of personal data. Inspection visits can be made by relevant employees after prior notification.

Any expenses incurred by the data controller in connection with a physical inspection shall be borne by the data controller itself. However, the data processor is obliged to allocate the resources (mainly the time) necessary for the data controller to carry out his inspection.

The Data Processor is entitled to reasonable remuneration for documented time spent at the hourly rate stated in the main agreement, and costs associated with the assistance regarding the abovementioned inspections written, physical or otherwise, unless otherwise agreed between the Parties.

### **C.8. Procedures for audits, including inspections, of the processing of personal data being performed by sub-processors.**

The data processor is responsible for carrying out the necessary supervision of the sub-processors. Documentation of the performed inspection can be sent upon request, to the data controller.

Based on the results of the documentation submitted, the data controller is entitled to request the implementation of additional measures to ensure compliance with the GDPR, data protection provisions of other EU member states, or national law and this DPA.

The Data Processor is entitled to reasonable remuneration for documented time spent at the hourly rate stated in the main agreement, and costs associated with the assistance regarding the abovementioned inspections written, physical or otherwise, unless otherwise agreed between the Parties.

## **Appendix D - The parties' terms of agreement on other subjects**

### **D.1 Derogation from standard clauses**

The paragraph below, has been deleted from the standard contractual clauses and does not apply to this agreement.

The data processor shall agree a third-party beneficiary clause with the sub-processor where – in the event of bankruptcy of the data processor – the data controller shall be a third-party beneficiary to the sub-processor agreement and shall have the right to enforce the agreement against the sub-processor engaged by the data processor, e.g., enabling the data controller to instruct the sub-processor to delete or return the personal data.

### **D.2 Remuneration to the data processor**

The Data Processor is entitled to reasonably and documented remuneration for time spend at the hourly rate stated in the main agreement, for documented and reasonable costs associated with changes and/or assistance to the Data Controller, unless otherwise agreed between the Parties.