LICENCE TERMS

Karnov Group Denmark A/S

Version 3.2

1. Introduction

The License Terms set out the terms and conditions that apply to the licensing of Karnov Group Denmark A/S' (Karnov Group) Licensed Product(s). If the Licensee purchases additional Licensed Products from the Licensor, such Licensed Products are automatically covered by the License Terms, unless separate terms apply to the purchased products.

1.1 Definitions

The License Terms use the following definitions:

"The Customer Agreement"	The agreement of the parties as issued at the time of the conclusion of the agreement including these License Terms.
"Licensor"	Karnov Group Denmark A/S
"Licensee"	The entity that has entered into an agreement with the Licensor for the supply of the Licensed Product(s).
"Users"	Anyone who has access to the Licensed Product, including employees, students and other users.
"Licensed Product(s)"	The Licensor's products for which the Licensee pays a License Fee, and which are subject to these License Terms.
"License Right"	The Licensee's right to use the Licensed Product(s), which the Licensee obtains upon acceptance of the License Terms and payment of the License Fee associated with the License, cf. section 2.1 of the License Terms and the appendices attached to the Customer Agreement.
"License Terms"	These License Terms, appendices thereto and any subsequent additions or changes, including price changes, cf. section 13 of the License Terms.
"License Fee"	The fee paid by the Licensee for access to the Licensed Product(s) during the subscription period
"Subscription Period"	The period during which the Licensee has purchased access to the Licensed Product(s)

2. Scope of License

2.1 Right of Use to the Licensed Product(s)

Upon acceptance of the License Terms and payment of the License Fees, the Licensee obtains a time-limited, non-transferable and non-exclusive right to use the Licensed Product(s) and any subsequent updates to the Licensed Product(s) in accordance with the License Terms.

The Right of Use entitles the Licensee, among other things, to perform, in connection with the usual use of the Licensed Product(s), the following actions, among others:

- to conduct searches
- to print physically and electronically
- to make electronic copies to documents outside of the Licensed Product(s),
- to copy physical content for internal use by Licensee
- to share content with other the Licensee's other Users
- to download parts of the Licensed Product(s)
- to add notes for the User(s) or the company's use, where possible
- to create notifications about new and changed content in the Licensed Product(s)
- create folders for relevant documents that can be shared with the Licensee's other User(s)

Additional rights of use may follow from the License Terms for separately Licensed Product(s), cf. the appendices attached to the License Terms.

Information and data constituting all or part of the Licensed Product(s) accessed by the Licensee may not be used in or for any business that competes with the Licensor's business areas at any given time.

The Licensed Product(s) or any part thereof may not be disclosed or otherwise made available to any third party. However, the Licensee may disclose collections of materials or the like to a third party, which the Licensee has compiled using the Licensed Product(s), if disclosure of such material is necessary for the Licensee's advice to clients, including in connection with disputes and in pleadings.

Unless expressly stated otherwise, the Licensee may not - and shall not permit any third party - to modify in any way the Licensed Product(s) or other materials provided by the Licensor.

2.2 Technical Prerequisites for Use of the Licensed Product(s)

The Licensee is responsible for obtaining and installing the necessary browser software for displaying the Licensed Product(s). The Licensee is aware that the possibilities of using the Licensed Product(s) depend on the Licensee's choice of browser software. The Licensor ensures that commonly used browsers are supported. The Licensee will be able to, on request, obtain information from the Licensor's Support, which browser software can be used to display the

Licensed Product(s). The Licensor is entitled to modify its software with the effect that the Licensee must acquire and install new browser software in order to be able to use the Licensed Product(s). The Licensee is also responsible for establishing a connection to the Licensor's server and for managing and maintaining this connection.

2.3 Compliance with the License Terms

The Licensee is obliged to ensure that the Licensee's Users are informed of and comply with the License Terms and respect the Licensor's intellectual property rights, including copyrights. The Licensee is always liable for the Users' use of the Licensed Product(s). The Licensee is responsible for keeping the login details of its Users confidential. For the avoidance of doubt, the Licensee is liable for any unauthorized use of the Licensed Product(s) caused by the Licensee or the Licensee's User(s) negligent handling of login details.

The Licensor conducts ongoing monitoring to ensure compliance with the License Terms. If the Licensor has reasonable grounds to suspect that the Licensee is in breach of these License Terms, the Licensee shall, upon the Licensor’s request, provide a written account of any circumstances relevant to assessing whether a violation has occurred.

2.4 Right of Withdrawal

If the Licensee is a consumer, the Licensee generally has 14 (fourteen) days to cancel the purchase of the Licensed Product(s), according to the Consumer Contracts Act. The Licensee acknowledges that any right of withdrawal ceases when the Licensed Product(s) is put into use. The Licensee thus agrees that the right of withdrawal can only be exercised until the time when the use of the Licensed Product(s) is activated. If the Licensee is not a consumer, the Licensee does not have the right to withdraw from the purchase of the Licensed.

3. Access to the Licensed Product(s)

Depending on the subscription type and scope of the Subscription as set put in the Customer Agreement, User access to the Licensed Product(s) will be granted through the options below.

The Licensee and its Users may not give third parties access to the Licensed Product(s). Furthermore, the Licensee and/or its User(s) may not disclose login details issued by the Licensor to third parties.

The Licensee may only grant access to the Licensed Product(s) to those Users to whom the Licensor has provided a personal account with associated login details in accordance with these License Terms. The Licensee shall not disclose or in any way divulge Users' login details to other employees or third parties.

3.1 Access via Personal Credentials

Entitled to use the Licensed is only the User(s) to whom the Licensor has issued personal credentials in accordance with the Agreement with the Licensee and the License Terms. A User may only log in to the Licensed Product(s) from three (3) devices at a time.

The Licensee and its User(s) may not disclose the password(s) issued by the Licensor.

3.2 Access via IP Address

An agreement can include access via the Licensee's IP address which allows the Licensee and its User(s) to access the Licensed Product(s) from the IP address approved by the Licensor.

If the agreement includes personal logins the Licensee's employees may have personal login credentials created by the Licensor. Personal login credentials are active until the termination of the Agreement or termination of the User(s) employment relationship. It is the Licensee's responsibility to inform the Licensor of a terminated employment relationship, as the right to use the personal login ceases by the date of termination of the employment relationship.

3.3 Access via Entra ID

User access to the Licensed Product(s) can be granted through the Licensee’s Microsoft Entra ID (Azure AD). All user creation, deactivation, and permission assignments are managed centrally by the Licensee’s own IT department, leveraging their existing identity governance policies. It is the Licensee's responsibility to ensure that user access ceases by the date of termination of the employment relationship.

4. Updating and Modifying the Licensed Product(s)

The Licensor has the right to update or modify the Licensed Product(s) on an ongoing basis, including features, functionality and content, when the Licensor deems it necessary. Such update or modification shall not entail any limitation or change in Licensee's obligations to the Licensor.

The Licensor may change or remove features of the Licensed Product(s) when needed to provide the best possible service to its customers. These changes do not affect the Licensee’s obligations or give the Licensee any right to any remedies. Removal of essential features constitutes a change to the License Terms, cf. Section 13.

5. Rights and Entitlements

5.1 Rights to the Licensed Product(s)

The Licensor, or any third party from whom the Licensor derives its rights, holds copyright and any other rights to the Licensed Product(s), including, but not limited to, html-code, text, images or other elements that the Licensee may access through the Licensed Product(s)s. The copyright also includes any physical material, including user manuals and educational materials, provided by the Licensor to the Licensee. Furthermore, the Licensor reserves all rights to the content, including the right to utilize the content for text and data mining purposes, cf. section Article 4 of the European Digital Single Market directive (DSM) as well as national implementations of the directive.

The Licensee and its User(s) shall respect the rights of the Licensor, and the Licensee shall be liable, without limitation of amount, for any violation of those rights, including unauthorized disclosure of the Licensed Product(s) to third parties.

The Licensee or its User(s) may not breach or alter any security mechanisms, including security codes, nor change or remove any information in the Licensed Product(s) regarding rights, trademarks, product information or the like.

5.2 Right to User-Generated Material

The Licensee and its User(s) can create user-generated material in the Licensed Product(s). The Licensee and its User(s) are in control of the user-generated material. The Licensor does not use user-generated material prepared by the Licensee or its User(s) for its own purposes.

The Licensee agrees that the Licensor deletes all user-generated material prepared by the Licensee or its User(s) upon termination of the Customer Agreement, or termination of the employment relationship between a User and the Licensee in accordance with section 3.

The Licensee shall ensure that the Licensee's User(s) are informed that the user-generated material will be deleted upon termination of the Customer Agreement and upon termination of employment with the Licensee. The Licensor shall have no responsibility or liability for, and shall not be a party to, any disputes between the Licensee and its User(s) concerning rights to user-generated material or its deletion.

5.3 Right to Uploaded Documents

The rights to user uploaded documents in the Licensed Product(s) are governed separately in the Appendices, including the Data Processing Agreement, which shall prevail over any conflicting provisions of these License Terms or any other agreement.

6. Payment for the Licensed Product(s)

6.1 Payment Terms

The License fee is paid in advance for subscription periods of 12 (twelve)) months at a time. The Licensor's payment terms are 14 (fourteen) days from the date of invoice.

If the Licensee does not make payment within the specified payment deadline, the outstanding amount will accrue default interest in accordance with the rules in the at any time applicable interest law. In the event of a payment reminder, the Licensor reserves the right to charge a reminder fee.

The Licensor reserves the right to temporarily close access to the Licensed Product(s), if the Licensor does not receive timely payment of the license fee from the Licensee. The Licensee is not entitled to any remedies due to limitation of access caused by the Licensee's failure to pay the License fee.

6.2 Deregistration, Transfer of or Purchase of User Access

The Licensee is not entitled to any credit due to terminated user access during the Subscription Period. The Licensee has the option to transfer a terminated user access to another User during the remaining part of the subscription period.

The Licensee has the option of purchasing additional user access during the Subscription Period. Additional user access will be invoiced separately, and billing will cover the remaining part of the Subscription Period.

7. Correction of Errors

The content and functionality of the Licensed Product(s) is strictly limited to what is expressly stated in the applicable product specifications at any given time. The Licensed Product(s) is licensed on an "as is" and “as available” basis, without warranty of any kind. Licensor makes no guarantee that the availability of the Licensed Product(s) and the connection to the Licensed Product(s) will be uninterrupted and error-free.

The Licensor conducts regular testing of the Licensed Product(s) but cannot exclude that the Licensed Product(s) - like any other software made available online - contains errors and inexpediencies. Such errors do not constitute grounds for termination and do not entitle the Licensee to remedies or other remedies. The same applies to errors in the Licensed Product(s) content. The Licensor strives to ensure that all errors and inexpediencies in the Licensed Product(s) are corrected on an ongoing basis but makes no guarantee that all errors and inexpediencies will be corrected.

8. Support

The Licensee is entitled to support regarding the Licensed Product(s) from the Licensor's Support. During the Licensor's office hours, support is provided by the Licensor. At other times, the Licensor may provide support through a third party. Contact information can be found on www.karnovgroup.dk.

A response to an inquiry can be expected within 3 (three) working days. If an enquiry is of such nature that further investigation is required, the Licensee and/or User will be notified within 3 (three) working days with an estimate of when the enquiry can be answered.

9. Liability and Indemnity

The Licensor is liable for product damage in accordance with the provisions of the applicable product liability legislation that cannot be waived by agreement but disclaims product liability on any other basis.

In no event shall the Licensor be liable to the Licensee for any indirect or consequential loss arising in connection with the use of the Licensed Product(s), including but not limited to business interruption, loss of anticipated profits, loss and/or recovery of data, loss of goodwill and other consequential damages. The Licensor is never liable to the Licensee for errors in the Licensee's advice to third parties that are due to errors or omissions in the Licensed Product(s).

The Licensor's liability for loss or damage under the Customer Agreement may in no event exceed the amount paid by the Licensee to the Licensor for the subscription period during which the damage occurred.

The Licensor disclaims any liability for loss or damage that can be attributed to the Licensee's own connection to the Licensor's product, including lack of connection, system breakdown, etc. The same applies in relation to the Licensee's other IT equipment, browser, software, etc.

In the event of a breach of the License Terms by a Licensee and/or its user(s), the Licensee shall, in addition to any claims for compensation for unauthorized use of the Licensed Product(s), compensate the Licensor for all damages incurred by the Licensor as a result of such breach.

10. Force Majeure

Neither party shall be deemed liable to the other party under the Customer Agreement in respect of matters beyond its control which it should not have taken into account at the time of entering into the Customer Agreement nor should it have avoided or overcome, including but not limited to; war and mobilization, civil unrest, natural disasters, strikes, lockouts, failure of supplies of raw materials, epidemics, pandemics or other outbreaks of serious human disease, fire, damage to production equipment, disruption of general transport, including energy supply, and import and/or export bans. Circumstances at the premises of a party's supplier shall be deemed to be force majeure for that party pursuant to this section 10 if there is a corresponding obstacle for the supplier and the supplier should not have avoided or overcome it, possibly by using an alternative supplier.

11. Transfer

Neither party may assign its rights and obligations under the Customer Agreement to any third party without the written consent of the other party. However, the Licensor may, without the Licensee's consent, assign its rights and obligations under the Customer Agreement to a company within Karnov Group.

12. Duration and Termination

The License Terms is an integrated part of the Customer Agreement and is effective during the Subscription Period.

Termination of the Customer Agreement must, unless otherwise agreed, be made no later than 14 (fourteen) days before the end of the current Subscription Period. If a termination is not received in time, the Licensee will be bound for another Subscription Period. Termination must be made in writing via e-mail to Customer Service, e-mail: **kundeservice@karnovgroup.com**

If the Licensee or its User(s) do not comply with the License Terms, the Licensor is entitled to immediate termination of the Customer Agreement without notice. In such case, the Licensee is entitled to receive reimbursement for the remaining Subscription Period as defined in the Customer Agreement.

13. Amendment of Terms

13.1 Amendment of the License Terms

The Licensor may amend the License Terms at any time. Significant changes must be notified to the Licensee no later than 30 (thirty) days before the change takes effect, unless it relates to a change that is necessary for Karnov Group to comply with applicable law. The Licensor's notice to the Licensee shall indicate the changes made.

If the Licensee does not wish to be bound by the amended License Terms, the Licensee shall, within 30 (thirty) days of notification of the change, notify the Licensor in writing that the amended License Terms are not accepted. The Licensor will then consider the Customer Agreement terminated at the time of notification of the change to the License Terms. If the Licensee has not notified the Licensor within the notification period that the amendment to the License Terms is not acceptable, the Customer Agreement shall continue in accordance with the amended License Terms.

13.2 Price Adjustments

The Licensor may adjust prices in accordance with Section 13.1 for the subsequent Subscription Period, provided that the Licensor notifies the Licensee of the price change no later than 30 (thirty) days before the end of the current Subscription Period. Notice may be provided by including the updated price information on the invoice for the subsequent Subscription Period.

If the Licensee does not accept the price adjustments, the Licensee may terminate the Customer Agreement with effect at the end of the current Subscription Period by giving written notice to the Licensor within 14 (fourteen) days of the Licensor’s notification of the price adjustment.

14. Processing of Personal Data

14.1 Licensor as a Data Controller

In connection with the provision of the Licensed Product(s), the Licensor will collect and process information about the Licensee, including the usage of the Licensed Product(s) by its User (s). The Licensor will in addition process personal data, which the User(s) may enter the Licensed Product(s)

Unless expressly stated otherwise, the Licensor is an independent data controller and collects and processes personally identifiable information about User(s) to the extent necessary to provide the Licensed Product(s). The Licensor alone determines the purposes and means used when processing personal data, and it is the responsibility of the Licensor to ensure that personal data is processed in accordance with the rules of the European General Data Protection Regulation (GDPR) and the Data Protection Act. The Licensee and its User(s) can read more about the Licensor's processing of personal data as a data controller in the Licensor's privacy policy, which can be found here.

14.2 Licensor as a Data Processor

In cases where the Licensor acts as data processor under the GDPR, it will be clearly stated in the appendices to the specific Licensed Product(s) in these License Terms. When the Licensor acts as a data processor the data processing agreement in appendix 5 will apply.

15. The E-Commerce Act's Information Obligations

The Licensor complies with all the information obligations imposed on service providers by the Act on Services in the Information Society, including certain aspects of electronic commerce (the E-Commerce Act). However, in order not to complicate the communication between the Licensee and the Licensor, the application of sections 10, 11(1) and 12 of the E-Commerce Act is waived to the greatest extent possible, cf. section 13(2) of the Act.

16. Confidentiality and Security

16.1 General Confidentiality

The Licensor and the Licensee agree to keep confidential and not to disclose to any third party any confidential information, data, or materials received from the other party in connection with this Customer Agreement, except where required by law or with prior written consent of the disclosing Party. Confidential information means all information, including technical, strategic and financial information, as well as all types of personal data, except for knowledge and know-how of a general nature, general and freely available public information.

16.2 Confidentiality on User Generated Material

User generated material in the Licensed Product(s) is treated with confidentially and is not disclosed to any unauthorized person. The Licensor further ensures that access to user-generated content is granted only to those employees for whom such access is necessary to perform their job duties.
The Licensor ensures that its employees who access user generated content are bound by confidentiality with regards to knowledge obtained in connection therewith.

16.2 Security

The Licensor ensures that user generated content is stored in a data environment that meets the security requirements for the storage of personal data, as described in Section 14 and where applicable, in the data processing agreement.

17. The Customer Agreement

The Customer Agreement consists of the parties' written agreement (agreement, receipt, e-mail or other written documentation) and the License Terms including appendices applicable at any given time.

In the event of doubts of interpretation, the following order of precedence between the documents shall apply:

1. The Customer Agreement (agreement, receipt, e-mail or other written documentation)
2. License terms

18. Applicable Law and Jurisdiction

The Customer Agreement is subject to Danish law. Any dispute that may arise in connection with the Customer Agreement, including disputes regarding the existence or validity of the Customer Agreement, shall be decided by the City Court of Copenhagen.

APPENDIX 1: SPECIFIC LICENSE TERMS FOR COLLECTION OF RECORDS

1. Use of Collections of Records

The Collection of Records gives the Licensee and its User(s) the right to compile electronic collections of materials for use in litigation and arbitration. The Collection of Records is built up of literature and practice that the Licensee and its User(s) access via the Licensed Product, as well as of literature and practice that the Licensee and its User(s) themselves upload to the service in the form of PDF documents.

The Collection of Records may only be used by the Licensee and its User(s) to compile a material collection consisting of literature and practice for use in litigation and arbitration. Thus, it is not permitted to use the Collection of Records for other forms of document storage or compilation of documents, including for the preparation of extracts.

If any literature or practice that the Licensee or its User(s) upload to the Collection of Records contains personal data, it is the Licensee's responsibility to ensure that the personal data is anonymised in accordance with applicable data protection legislation. The Licensor thus does not act as a data processor for the Licensee.

The Licensee and its User(s) may not use outputs from the Licensed Product(s) in any manner that:

- Is incorrect or misleading;
- Infringes any third party's copyright, right of publicity, patent, trademark, trade secret, or other rights, including rights to privacy;
- Violates any applicable law, government regulation, or court order (including, but not limited to, those governing export control, consumer protection, unfair competition, anti-discrimination, or misleading advertising);
- Is, or could reasonably be considered, defamatory, libelous, hateful, racially or religiously biased or offensive, or unlawfully threatening or harassing to any individual, partnership, or company;
- contains viruses or is suitable for distributing malware;
- damage the Collection of Records or impair anyone else's use of the Collection of Records;
- Assists or encourages others to commit any of the above acts.

2. Indemnification

The Licensee agrees to indemnify the Licensor for all claims arising from a breach of the Licensee's warranty pursuant to the last paragraph of Section 1.

3. Consequences of using the Collection of Records in violation of the License Terms

The Licensor reserves the right to change, block or delete any content that the Licensee uploads to the Collection of Records and that the Licensor in its sole discretion deems to be in violation of the Customer Agreement. In this connection, the Licensee accepts that the Licensor monitors compliance with the License Terms and that the Licensor in this connection obtains insight into material uploaded to the Collection of Records.

Suspicion or violation of this may result in the suspension of the Collection of Records and termination of the Customer Agreement with the Licensee. Unless the Licensor believes that immediate suspension is required, the Licensor will provide reasonable notice prior to suspension of the Collection of Records and termination of the Customer Agreement.

4. Rights to Collections of Records

The Licensee and its User(s) acquire the rights to the Collection of Records that they create in connection with the use of the Collection of Records for such purposes as the Licensee may deem necessary. It is the responsibility of the Licensee and its User(s) to agree on the mutual distribution of the rights. Any dispute regarding this is thus irrelevant to the Licensor.

5. Availability

The Licensee acknowledges that the Licensor will delete material uploaded to or created by the Licensee or its User(s) in the Collection of Records upon termination of the Agreement, and that material uploaded to or created by individual User(s) in the Collection of Records will be deleted upon termination of the employment relationship between the User in question and the Licensee.

The Licensor is not in any way responsible for the availability of Collections of Records created in the Collection. It is thus the responsibility of the Licensee and its User(s) to ensure that the Collections of Records and documents that are to be preserved are stored securely on the Licensee's own systems or otherwise stored so that they are always available to the Licensee. Nor is the Licensor responsible for any loss and/or corruption of documents in the Collection of Records, regardless of the reason for this.

APPENDIX 2: SPECIFIC LICENCE TERMS FOR KARNOV KOMMUNE

1. Use of Karnov Kommune

Karnov Kommune is an information solution designed for caseworkers and other professionals. The platform provides resources including guides for case processing, annotated laws and regulation, case law and more. User(s) can submit questions to legal experts. Additionally, authorized User(s) may upload internal documents, such as policies and guidelines, which will be available to all the Licensee's User(s) of the Licensed Product

2. Upload Functionality for the Licensee's Internal Documents

The Licensee and its User(s) may upload their internal documents to the Licensed Product. Uploaded documents are only accessible to the Licensee's User(s). The Licensee agrees that it is the Licensee's responsibility to ensure that their User(s) documents uploaded to the Licensed Product are suitable for that purpose. The supported document formats for upload are determined by the Licensor.

If part of the Customer Agreement, the Licensee may have the option to make its internal documents available as a data source to the Licensor's AI-functionality, by marking it at upload.

The Licensee acknowledges that the Licensor may monitor compliance with these License Terms and, in doing so, may access material uploaded to the Licensed Product.

2.1 Permitted Use of the Upload Functionality

The Licensee and its User(s) are permitted to use the upload function to add internal resources—such as guidelines, policies, or procedural documents—that may guide or support their work within the Licensed Product, including legal analysis and quality assurance activities.

The Licensee and its User(s) guarantee that any material uploaded to the Licensed Product will not:

- be incorrect or misleading.
- infringe any third party's copyright, rights of publicity, patent, trademark, trade secret, or other rights, including privacy rights;
- violate any applicable law, government regulation, or court order (including, but not limited to, provisions governing export control, consumer protection, unfair competition, anti-discrimination, or misleading advertising);
- be, or could be reasonably considered libelous, defamatory, hateful, racially, or religiously biased or offensive, unlawfully threatening, or harassing toward any individual, partnership, or company;
- contain viruses or be suitable for distributing malware;
- damage the Licensed Product or impair others' use of the Licensed Product;
- assist others, or encourage them, to perform any of the above actions.

If the Licensee or its User(s) need to upload documents containing personal data, they must ensure that such data is anonymized in accordance with applicable data protection legislation prior to upload.

2.2. Indemnification

Licensee agrees to indemnify Licensor for all claims arising from a breach of Licensee's warranty under Section 2.1.

2.3. Consequences of Improper Use of the Upload Functionality

The Licensor reserves the right, at its sole discretion to change, block or delete any content uploaded to the Licensed Product by the Licensee if such content is found to violate the Customer Agreement.

The Licensee accepts that the Licensor monitors compliance with the License Terms and that the Licensor in that regard obtains access to the materials uploaded to the Licensed Product.

If the Licensor suspects or determines a violation of these License Terms it may suspend certain functionalities or terminate the Customer Agreement with the Licensee. Unless immediate suspension is deemed necessary, the Licensor will provide reasonable notice before suspending functionality or terminating the Customer Agreement.

2.4 Availability of Uploaded Documents

The Licensor is not responsible for the continued availability of documents uploaded or otherwise stored in the Licensed Product. It is the Licensee's responsibility to ensure that documents to be preserved are securely stored on the Licensee's own systems or otherwise maintained so they are always available to the Licensee. The Licensor is not responsible for any loss or corruption of documents in the Licensed Product, regardless of the cause.

Upon termination of the Customer Agreement, the Licensor agrees to provide all documents uploaded to Licensed Product by the Licensee or its User(s) to the Licensee.

3. "Ask the Expert"

The Licensee and its User(s) may submit legal questions via an online form. The questions may not contain personally identifiable data.

3.1 Nature of the Questions

"Ask the Expert" only covers legal issues relevant to the area to which the feature pertains. The feature is not meant for individual assessments, and the questions must be substantial and should not concern matters where the answer can be found via a simple search in the Licensor's Licensed Products.

If a submitted question does not meet the conditions for permitted use of the feature, the Licensor or the Licensor's experts may refrain from answering. If appropriate, the Licensee or its User(s) may be asked to reformulate, specify, or delimit the question. The Licensor reserves the right to publish submitted questions, and in connection with this, may shorten or otherwise edit the question prior to publication.

3.2 Replies

Submitted questions are usually answered within 72 hours, either in writing or by telephone. A selection of questions and corresponding answers may be published in "Ask the Expert" so that other users can benefit from questions of a general nature. All questions and answers are anonymized before publication.

3.3 Disclaimer

The "Ask the Expert" feature does not constitute legal advice, case processing, or provide binding answers. Any information or responses are for general informational purposes only and are not a substitute for professional advice in specific cases. The Licensor assumes no responsibility for any financial or other consequences resulting from the use of, or reliance on, information provided through this feature, including any misleading or incorrect information. In no event shall the Licensor or its experts be liable to the Licensee or its User(s) for any direct, indirect, or consequential damages (including loss, loss of anticipated profits, loss of goodwill, or other similar consequential damages) arising from the use of, or reliance on, the "Ask the Expert" feature.

3.4 Processing of Personal Data

The Licensee’s Users’ personal data will be stored in the Licensor's systems for up to two years, in accordance with Article 6(1)(f) of the General Data Protection Regulation.

3.5 Accessibility of “Ask the Expert”

The Licensor is not responsible for the continued availability of documents published or otherwise stored in the Licensed Product. It is the Licensee’s responsibility to ensure that documents to be preserved are securely stored on the Licensee’s own systems or otherwise maintained so they are always available to the Licensee.

The Licensor is not responsible for any loss or corruption of documents in the Licensed Product, regardless of the cause.

4. "Karnov Guides"

4.1 Rights to Results and Documents Prepared in Karnov Guides

As part of the Licensed Product, the Licensee and its User(s) have the opportunity to make calculations and, on the basis of the information entered, to access standard company documents and letters, which have been corrected on the basis of the information entered.

The Licensee and its User(s) acquire the rights to the results and documents produced by the Licensee and its User(s) in connection with the use of the Licensed Product for the purposes that Licensee may deem necessary. It is the responsibility of the Licensee and its Users to agree on the detailed distribution of the rights among themselves. Any dispute regarding this is therefore irrelevant to the Licensor.

However, the Licensor retains all rights to the formulas, calculation methods and the like that form the basis for the calculations that the Licensee may make in the Licensed Product.

4.2 Accessibility

Results and documents generated by the Licensee or its User(s) in the Licensed Product will be deleted after 1 year from the date of creation, unless the Licensee or its User(s) themselves delete results or documents in the Licensor's system.

The Licensee agrees that it is not possible to upload documents to the Licensed Product.

The licensor is not in any way responsible for the availability of results and documents produced in the Licensed Product. It is thus the responsibility of the Licensee and its User(s) to ensure that the results and documents that are to be preserved are stored securely on the Licensee's own systems or otherwise stored so that they are available to the Licensee at all times.

Nor is the licensor liable for any loss and/or corruption of results or documents in the Licensed Product for any reason.

Licensee agrees that Licensor will delete all results and documents generated in the Licensed Product by Licensee or its Users upon termination of the Customer Agreement, and that individual Users' results and documents will be deleted upon termination of the employment relationship between the User and the Licensee in question.

1. Using KAILA

KAILA is an information solution for case workers and other professionals who require access to legal materials and analysis in their work. The solution combines resources from the Licensor's Licensed Products – including uploaded internal documents, annotated laws and regulations, case law, online library, and other legal materials - to support legal research and analysis. Users can leverage KAILA's tools to efficiently search, help analyze or interpret legal information relevant to their legal research.

2. Acceptable Use of KAILA

The Licensee and its User(s) have unlimited access to KAILA, subject to compliance with these License Terms. The Licensor continuously monitors usage patterns and reserves the right to impose usage caps in the event of suspected misuse. The Licensee is responsible for ensuring that its User(s) utilize the Licensed Product in accordance with these License Terms.

The Licensed Product may not be used for activities such as:

- Automating or repeating requests;
- Manipulating the system to circumvent restrictions;
- Taking actions that may harm the performance or integrity of the Licensed Product;
- Attempting to access the Licensed Product's source code or algorithms;
- Modifying the Licensed Product's software using techniques such as reverse engineering or decompiling, in whole or in part;
- Modifying or distributing any part of the Licensed Product in a way that infringes upon the Licensor's rights, including intellectual property rights;
- Damages the Licensed Product or impairs others' use of the Licensed Product;
- Circumventing or violating any security mechanisms within the Licensed Product;

The Licensee and its User(s) shall not enter personal data into the Licensed Product.

The Licensed Product shall not be used for the purpose of making decisions based solely on automated processing, including profiling, which produces legal effects concerning the data subject or similarly significantly affects the data subject. The Licensee is responsible for ensuring that the system is not used for such purposes.

The Licensee and its User(s) may not use outputs from KAILA in any manner that:

- Is incorrect or misleading;
- Infringes any third party's copyright, right of publicity, patent, trademark, trade secret, or other rights, including rights to privacy;
- Violates any applicable law, government regulation, or court order (including, but not limited to, those governing export control, consumer protection, unfair competition, anti-discrimination, or misleading advertising);
- Is, or could reasonably be considered, defamatory, libelous, hateful, racially or religiously biased or offensive, or unlawfully threatening or harassing to any individual, partnership, or company;
- Assists or encourages others to commit any of the above acts.

The Licensee may not use knowledge gained from the Licenced Product, or any part thereof, in activities that compete with the Licensor's business.

3. Training in the Use of KAILA

The Licensor has an exclusive right to teach the use of the Licensed Product, including for public performance. Courses or similar events about the Licensed Product may therefore not take place without the prior specific consent of the Licensor.

4. Third Party Rights and Unlawful Content

To the extent that content available via the Licensor's Licensed Product(s), or output generated by the Licensed Product, is subject to third-party intellectual property rights, the Licensee must comply with all applicable laws and regulations governing the copying and use of such content.

The Licensee or the User(s) inputs (prompts) and the outputs generated therefrom must respect the rights of third parties, including intellectual property rights, and comply with applicable law at all times. The Licensee agrees that it is its responsibility to ensure that User(s) within the Licensee's organization use the product only in accordance with the License Terms.

5. Liability & Indemnification

The Licensee agrees to indemnify and hold harmless the Licensor against any and all claims, damages, losses, or expenses arising from a breach by the Licensee or its User(s) of the obligations set forth in Sections 2-4 of this appendix.

6. Consequences of Unauthorized Use

The Licensor reserves the right to change, block or delete any content that the Licensee generates through the Licensed Product and that the Licensor deems in its sole discretion to be in violation of the Customer Agreement. In this connection, the Licensee accepts that the Licensor controls compliance with the license terms, and the Licensor in this connection gains insight into the User(s) input and output data.

In the event of repeated or deliberate breaches of the above, the Licensor may:

- Suspend or terminate the User(s) access without further notice; and/or
- Temporarily restrict access to the Licensed Product; and/or
- Terminate the Customer Agreement with the Licensee

Unless the Licensor believes that immediate suspension is required, the Licensor will provide reasonable notice prior to suspension of functionality and/or termination of the Customer Agreement.

7. Disclaimer

The use of the Licensed Product does not equate to legal advice, case management, binding answers, or similar services. Outputs from the Licensed Product are to be considered indicative only and must always be independently verified by the Licensee and/or its User(s).

The Licensor assumes no responsibility for any financial or other consequences resulting from the information provided by the Licensed Product or its use. The Licensor further disclaims any liability for misleading or incorrect information provided by the Licensed Product. In no event shall the Licensor be liable to the Licensee or its User(s) for any direct, indirect, or consequential damages (including loss, loss of anticipated profits, loss of goodwill, or similar consequential damages) arising from use of the Licensed Product.

The Licensor is not responsible for downtime or technical issues that may affect the availability of the Licensed Product.

8. Uploaded Documents as a Data Source

When used by the Licensee's User(s), the Licensed Product can access the Licensee's Internal Documents uploaded cf. appendix 2 as a data source, provided that the Licensee has made the documents accessible to the Licensed Product at upload.

9. The Licensor's Processing of Data

The Licensee or its User(s) personal data will be processed in accordance with the Licensor's License Terms section 14.1 (Licensor as a Data Controller), section 14.2 (Licensor as a Data Processor) and the Data Processing Agreement in appendix 5.

If The Licensor or its User(s) provides feedback in the Licensed Product and thereby has given consent to disclose information to the Licensor, the Licensor reserves the right to use the User(s) input, output and other data regarding the use of the Licensed Product to improve the solution in anonymized form.

10. Availability of User Data

The Licensee accepts that the Licensor stores User conversations within the Licensed Product. For conversations that are not pinned by the User, each conversation will be available to the User for 90 days following the most recent activity and will then be deleted, unless deleted earlier by the User. Pinned conversations will be retained until they are either actively deleted by the User or until the termination of the Customer Agreement.

Upon termination of the Customer Agreement, all data relating to the User(s), including conversations within the Licensed Product, will be deleted by the Licensor.

The Licensor is not responsible for the continued availability of conversations. It is the responsibility of the Licensee to ensure that any output they wish to preserve are securely stored on their own systems or by other means, so they remain accessible at all times.

The Licensor is not liable for any loss or corruption of documents or data in the Licensed Product, regardless of the reason.

11. Changes

The Licensor reserves the right to update the License Terms for the Licensed Product, including to reflect changes in cost structure, technology, or user behavior. Unless otherwise stated below, any such changes will be communicated in accordance with Section 13 of the License Terms.

Notwithstanding the foregoing, the Licensor reserves the right, at its sole discretion, to replace, update, or otherwise modify the underlying large language model (LLM) without prior notice to the Licensee.

1. Use of AI Products

KAILA (JURA) and KAILA Flow are information and workflow solutions designed for legal professionals who require access to legal materials and tools for managing legal work. The solutions combine resources from the Licensor's Licensed Products—including annotated laws and regulations, case law, online library resources, and other legal materials—to support legal research, analysis, and legal workflows.

Users can leverage the Licensed Products to search, analyze, interpret, organize, and work with legal information relevant to their legal matters and professional activities. The solutions can also assist users in streamlining legal processes, managing tasks, generating work product, and supporting decision-making within legal workflows.

2. Acceptable Use of AI Products

The Licensee and its User(s) have access to the Licensed Product, subject to compliance with these License Terms. The Licensed Product includes functionality that enables individual User(s) to upload documents directly to the Licensed Product. Accepted file formats, number of files and file size are determined by the Licensor.

The Licensor continuously monitors usage patterns and reserves the right to impose further usage caps in the event of suspected misuse. The Licensee is responsible for ensuring that its User(s) utilize the Licensed Product in accordance with these License Terms.

The licensed Product may not be used for activities such as:

- Automating or repeating requests;
- Manipulating the system to circumvent restrictions;
- Taking actions that may harm the performance or integrity of the Licensed Product;
- Attempting to access the Licensed Product's source code or algorithms;
- Modifying the Licensed Product using techniques such as reverse engineering or decompiling, in whole or in part;
- Modifying or distributing any part of the Licensed Product in a way that infringes upon the Licensor's rights, including intellectual property rights;
- Damages the Licensed Product or impairs others' use of the Licensed Product;
- Circumventing or violating any security mechanisms within the Licensed Product;

The Licensed Product shall not be used for the purpose of making decisions based solely on automated processing, including profiling, which produces legal effects concerning the data subject or similarly significantly affects the data subject. The Licensee is responsible for ensuring that the system is not used for such purposes.

The Licensee and its User(s) may not use outputs from the Licensed product(s)s in any manner that:

- Is incorrect or misleading;
- Infringes any third party's copyright, right of publicity, patent, trademark, trade secret, or other rights, including rights to privacy;
- Violates any applicable law, government regulation, or court order (including, but not limited to, those governing export control, consumer protection, unfair competition, anti-discrimination, or misleading advertising);
- Is, or could reasonably be considered, defamatory, libelous, hateful, racially or religiously biased or offensive, or unlawfully threatening or harassing to any individual, partnership, or company;
- Assists or encourages others to commit any of the above acts.

The Licensee may not use knowledge gained from the Licensed Product, or any part thereof, in activities that compete with the Licensor's business.

3. Training in the Use of Licensed Products

The Licensor retains the exclusive right to offer and provide commercial training services on the use of the Licensed Product, including public presentations or demonstrations offered to third parties for a fee or other commercial benefit.

4. Third Party Rights and Unlawful Content

To the extent that content available via the Licensor's Licensed Products, or output generated by the Licensed Product, is subject to third-party intellectual property rights, the Licensee must comply with all applicable laws and general legal rules governing the copying and use of such content.

The Licensee and its User(s) are responsible for ensuring that both inputs (prompts) and outputs generated via the Licensed Product respect third-party rights, including but not limited to intellectual property, and that such use always complies with applicable laws and regulations.

5. Liability and Indemnification

The Licensee agrees to indemnify and hold harmless the Licensor against any and all claims, damages, losses, or expenses arising from a breach by the Licensee or its User(s) of the obligations set forth in Sections 2 – 4 of this Annex.

6. Consequences of Unauthorized Use

The Licensor reserves the right to modify, block, or delete any content generated by the Licensee through the Licensed Product if, in the Licensor's sole discretion, such content is found to be in violation of the Customer Agreement. The Licensee acknowledges that the Licensor may monitor compliance with these License Terms and, in this context, may access User input and output data.

In the event of repeated or wilful violations, the Licensor may:

- Suspend or terminate the User(s) access without further notice; and/or
- Temporarily restrict access to the Licensed Product; and/or
- Terminate the Customer Agreement with the Licensee.

Unless the Licensor believes that immediate suspension is required, the Licensor will provide reasonable notice prior to suspension of functionality and/or termination of the Customer Agreement.

7. Disclaimer

The use of the Licensed Product does not equate to legal advice, case management, binding answers, or similar services. Outputs from the Licensed Product are to be considered indicative only and must always be independently verified by the Licensee and/or its User(s).

The Licensor assumes no responsibility for any financial or other consequences resulting from the information provided by the Licensed Product or its use. The Licensor further disclaims any liability for misleading or incorrect information provided by the Licensed Product. In no event shall the Licensor be liable to the Licensee or its User(s) for any direct, indirect, or consequential damages (including loss, loss of anticipated profits, loss of goodwill, or similar consequential damages) arising from use of the Licensed Product.

The Licensor is not responsible for downtime or technical issues that may affect the availability of the Licensed Product.

8. The Licensor's Processing of Data

The Licensee or its User(s) personal data will be processed in accordance with the Licensor's License Terms section 14.1 (Licensor as a Data Controller), section 14.2 (Licensor as a Data Processor) and the Data Processing Agreement in appendix 5.

If The Licensor or its User(s) provides feedback in the Licensed Product and thereby has given consent to disclose information to the Licensor, the Licensor reserves the right to use the User(s) input, output and other data regarding the use of the Licensed Product to improve the solution in anonymized form.

9. Availability and Use of Data

The Licensee acknowledges that the Licensor stores User conversations and uploaded documents within the Licensed Product. For conversations that are not pinned by the User, each conversation will be available to the User for 90 (ninety) days following the most recent activity and will then be deleted, unless deleted earlier by the User. Pinned conversations will be retained until they are either actively deleted by the User or until the termination of the Customer Agreement.

Upon termination of the Customer Agreement, all data relating to the User(s), including conversations within the Licensed Product, will be deleted by the Licensor.

The Licensor is not responsible for the continued availability of conversations. It is the responsibility of the Licensee to ensure that any output they wish to preserve are securely stored on their own systems or by other means, so they remain accessible at all times.

The Licensor is not liable for any loss or corruption of documents or data in the Licensed Product, regardless of the reason.

11. Changes

The Licensor reserves the right to update the terms of use of the Licensed Product(s) to reflect changes in our cost structure, technology or user behaviour. Any changes will be communicated as stated in the Licensor's License Terms section 13.

Notwithstanding the foregoing, the Licensor reserves the right, at its sole discretion, to replace, update, or otherwise modify the underlying large language model (LLM) without prior notice to the Licensee. In such cases, the Licensor shall ensure that the processing of personal data continues to meet at least the same level of security as was in place at the time of entering into the Customer Agreement, in accordance with the provisions of these License Terms including the data processing agreement in Appendix 5.

APPENDIX 5: DATA PROCESSING AGREEMENT

Version 1.1

This Data Processing Agreement (DPA) supplements the Customer Agreement, or other Agreement in place between Customer and Karnov Group[1] covering the Customer's use of Karnov Group Licensed Product(s).

This DPA is between the Customer (Data Controller) and the contracting party in the Customer Agreement will act as a Data Processor, and hereafter the companies are referred to jointly as Karnov Group (Data Processor).

[1] Meaning the relevant entity within Karnov Group, which the Customer has entered into an Agreement with

Table of Contents

1 Preamble 28
2 The rights and obligations of the Data Controller 29
3 The Data Processor acts according to instructions 29
4 Confidentiality 29
5 Security of processing 30
6 Use of sub-processors 31
7 Transfer of data to third countries or international organisations 32
8 Assistance to the data controller 32
9 Notification of personal data breach 33
10 Erasure and return of data 34
11 Audit and inspection 34
12 The parties' agreement on other terms 35
13 Commencement and termination 35
14 Amendment of the Data Processing Agreement 35

Appendix A - Information about the processing 36
Appendix B - Authorised sub-processors 38
Appendix C - Instruction pertaining to the use of personal data 40

1 Preamble

1.1 This DPA 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 DPA has 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 with regard to 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 the Licensed Product(s), the Data Processor will process personal data on behalf of the Data Controller in accordance with the DPA.

1.4 The DPA covers the Licensed Product(s) provided by Karnov Group.

1.5 Three appendices are attached to the DPA and form an integral part of the DPA and the DPA shall take priority over any similar provisions contained in other agreements between the parties.

1.6 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.

1.7 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.

1.8 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.

1.9 The DPA along with appendices shall be retained in writing, including electronically, by both parties.

1.10 The DPA 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[2] data protection provisions and the DPA.

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 DPA.

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. Based on 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.

[2] References to" Member States" made throughout the DPA shall be understood as references to "EEA Member States".

5 Security of processing

5.1 Article 32 GDPR stipulates that, considering 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.

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:

a. Pseudonymisation and encryption of personal data;

b. the ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;

c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

d. a process for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

5.2 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.

5.3 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.

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

6.2 The Data Processor shall meet the requirements specified in Article 28(2) and (4) GDPR to engage another processor (a sub-processor).

6.3 The Data Processor shall therefore not engage another processor (sub-processor) for the fulfilment of the DPA without the prior general written authorisation of the Data Controller.

6.4 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 **60 (sixty) days** 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.

6.5 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 DPA 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 DPA and the GDPR.

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 DPA 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 DPA are imposed on the sub-processor. Conditions 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 DPA:

a. transfer personal data to a data controller or a data processor in a third country or in an international organization

b. transfer the processing of personal data to a sub-processor in a third country

c. have the personal data processed in by the data processor in a third country

7.4 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.

7.5 The DPA shall not be confused with standard data protection clauses within the meaning of Article 46(2)(c) and (d) GDPR, and the DPA 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, 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 communicates 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, 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 48 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 8(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, 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 DPA 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 on other terms concerning the provision of the personal data processing specifying e.g., liability, if they do not contradict directly or indirectly the DPA 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 DPA is an integrated part of the Customer Agreement between the Data Processer and the Data Controller and shall become effective on the date of acceptance of that.

13.2 Both parties shall be entitled to require the DPA renegotiated if changes to the law or inexpediency of the DPA should give rise to such renegotiation.

13.3 The DPA shall apply for the duration of the provision of personal data processing. For the duration of the provision of personal data processing, the DPA cannot be terminated unless another DPA governing the provision of personal data processing services have been agreed between the parties.

13.4 If the provision of personal data processing is terminated, and the personal data is deleted or returned to the data controller pursuant to Clause 11.1. and Appendix C.4., the DPA may be terminated by written notice by either party.

14 Amendment of the Data Processing Agreement

14.1. The Data Processor may change the DPA at any time, and the Data Processor has to ensure that the Data Controller is notified no later than 30 (thirty) days before the change takes effect, unless it relates to a change that is necessary for the Data Processor to comply with applicable law and where a shorter notice period is necessary to ensure compliance with the law. The Data Processors notice to the Data Controller shall indicate the changes made.

14.2. If the Data Controller does not wish to be bound by the amended DPA, the Data Controller shall, within thirty (30) days of notification of the change, notify The Data Processor in writing that the amended DPA are not accepted. The Data Processor will then consider the Customer Agreement terminated at the time of notification of the change to the DPA.

14.3. If, within 30 (thirty) days of notification of the change, The Data Controller has not notified The Data Processor that the amendment to the DPA is not acceptable, the DPA shall continue in accordance with the amended DPA.

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 provides the Licensed Product(s) used by the Data Controller. The purpose of the processing applies to all Licensed Products provided by the Data Processor, where it is possible to write, upload or otherwise include customer data that includes personal data.

The Data Controller can use the Licensed Product(s) provided by The Data Processor, which is owned and managed by The Data Processor, to process information contained in the Data Controllers internal documents and cases in order for the Data Controller to get access to articles, notes, legislation and casework which is needed to solve their tasks.

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)

The Licensed Product(s) provided by the Data Processor can be used to collect, process and store personal information, provided by the Data Controller. 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 Data Processor may receive and process personal information under the terms of this DPA.

The Data Processor acknowledges that, depending on The Data Controller's use of the Licensed Product(s), The Data Controller may elect to include personal data from any of the following types of personal data:

Name, address, telephone number, e-mail, date of birth, CPR number, ID numbers, position, salary, pay slips, bank information, tax information, insurance data, union membership, health information, disciplinary actions, notes from job interviews, child protection cases, guardianship, criminal offences, photos, video footage, medical records, sexual relationships and orientation, social security status, financial and social issues, contracts, and documents containing confidential and sensitive personal data (and any other personal data including according to articles 6, 9, and 10 of the GDPR).

A.4. Processing includes the following categories of data subject

The Data Processor acknowledges that, depending on The Data Controller's use of the Licensed Product(s), The Data Controller may elect to include personal data from any of the following types of data subjects in the personal data:

- management, employees, and advisors,
- customers of the Data Controller and other third parties whose information may prove relevant in connection with the Data Controllers' use of the Licensed Product(s).

- information about parties in cases or other internal documents whose information appears in such documents that the Data Controller chooses to upload to the Licensed Product(s).

The abovementioned list is a non-exhaustive list, and the Data Controller has the overall responsibility to ensure that it has the right to process the personal data, which is uploaded to the Licensed Product(s) provided by the Data Processor.

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 DPA commence. Processing has the following duration

The processing is not time-limited and lasts until the Customer Agreement and DPA is terminated by one of the Parties.

Appendix B - Authorised sub-processors

B.1. Approved sub-processors

On commencement of the DPA, the Data Controller authorises the engagement of the following sub-processors:

NAME	PROCESSING LOCATION	DESCRIPTION OF PROCESSING	SECURITY MEASURES	SUB-SUBPROCESSERS
Azure by Microsoft	Microsoft European data centers in the Netherlands & Ireland	**Cloud hosting provider.**	**Azure documentation | Microsoft Learn**	Link to sub-sub processors: Service Trust Portal Home Page
Microsoft Foundry	Microsoft European data centers in Sweden	**Generative AI service provider for functionality capabilities.**	**Data, privacy, and security for Azure OpenAI Service - Azure AI services | Microsoft Learn**	Link to sub-subprocessors: Service Trust Portal Home Page
Google Cloud Platform	Google European Datacentres in Germany & the Netherlands	**Cloud hosting provider.**	**Security | Google Cloud**	Link to sub-subprocessors: Google Cloud Platform Sub processors | Google Cloud
Gemini Enterprise Agent Platform	Google European Datacentre in Germany	**Generative AI service provider for functionality capabilities.**	**Security controls for Vertex AI | Google Cloud**	Link to sub-subprocessors: Google Cloud Platform Sub processors | Google Cloud

The Data Controller shall on the commencement of the DPA 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-processer or change of processing activities must be received by the data controller at least **60 (sixty) days** prior to the application or change will commence.

The Data Controller has the right to object to the proposed change within **30 (thirty) days** of receiving the notification. An objection must be in writing and substantiated, and it must specify why the proposed change is considered to be in conflict with the GDPR or the current DPA.

If the Data Controller submits a relevant and justified objection that cannot be resolved through dialogue between the parties, the Data Controller may choose to terminate the DPA in line with the relevant section of the Customer Agreement.

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 provides the Licensed Product(s), where personal information can be entered, processed, and stored according to the Customer Agreement. The Data Processor may only process such personal data to the extent necessary to provide the Licensed Product(s).

The Data Processor may upon consent by the users from the Data Controller access personal information in relation to feedback, guidance or other support where it is necessary for the Data Processor to access the data in order to provide the Licensed Product(s).

In cases where the Data Processor has reasonable suspicion of misuse of the Licensed Product(s) such as fraud, infringement of the terms and conditions of the data processor the data processor can access the data without notifying the data controller.

In cases where the Data Processor uses generative AI services for the provision of the Licensed Product(s), the Data Processor ensures that data is not used for training of generative AI services, and that the processing of data is carried out exclusively for the purposes described in this DPA or the Customer Agreement.

The Data Processor must not process data for purposes outside of the Customer Agreement or this DPA without explicit, written consent from the Data Controller

C.2. Security of processing

Taking into account, the nature, scope and purposes of the processing activities as well as the risk for the rights and freedoms of natural person, the Data Processor shall maintain and implement appropriate technical and organisational measures to protect the Data Controllers data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.

The security measures will be aligned with the principles in ISO27001:2022 and ISO27701:2019 and will consist of the following areas:

Governance
Security responsibilities are formally defined and allocated across the organization. Policies are regularly reviewed and approved by management. An Information Security Board oversees compliance and risk management, and a Three Lines of Defense model ensures effective embedding and independent assurance of cyber and information security.

Human Resource Security
Personnel and third-party contractors are required to understand their information security responsibilities. Mandatory security awareness training is provided, and reference checks are conducted before access to systems is granted. Employment contracts include confidentiality

obligations, and personnel must adhere to relevant policies, including information security policy, Privacy policy, and Code of conduct.

Asset Management
All organizational assets - hardware, software, and data - are identified, tracked, and managed throughout their lifecycle. Secure disposal procedures ensure that decommissioned assets do not pose a data security risk, with destruction or sanitization of storage components to prevent unauthorized access to residual data.

Information Protection
Procedures and controls are implemented to safeguard confidentiality, integrity, and availability of information. Policies and technical measures ensure appropriate handling and security of data. All data, including personal data, is encrypted in transit and at rest.

Identity and Access Management
Role-based access controls are in place to ensure only authorized personnel can access systems and data. Permissions are based on least privileged access mechanisms and business needs, with regular reviews to maintain appropriate access levels.

Physical Security
Measures are implemented to secure data centers, offices, and infrastructure against unauthorized physical access, damage, or interference. Access to office premises is controlled via personal access cards, a Mobile Device Management (MDM) solution is implemented, and clear screen and removable storage instructions apply.

Security Management (Systems, Networks, Applications, Threats, Vulnerabilities, and Configurations)
Systems and infrastructure are monitored and managed to mitigate technical risks. This includes system hardening, regular updates, penetration testing, and application of security baselines to minimize vulnerabilities.

Supplier Relationships Security
Suppliers are assessed and classified based on the risk and type of information they process. Appropriate controls are defined to ensure compliance and security responsibilities throughout the supply chain.

Information Security Incident Management and Log Monitoring
A formal incident response plan ensures prompt detection, reporting, and resolution of security events. Security event monitoring and real-time alerting are managed, and logs are maintained for forensic analysis and incident investigation.

Continuity
Business continuity measures and disaster recovery plans are in place to ensure the ongoing availability of services in the event of disruptions.

Legal and Compliance
Compliance with legal, regulatory, and contractual requirements is maintained through regular review and implementation of relevant rules and standards.

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 all relevant information must be submitted to the Data Controller.

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 until termination of the Customer Agreement after which the personal data is erased by the Data Processor within 30 days. Furthermore, the Data Controller and its users can delete queries and documents.

Upon termination of the provision of the Licensed Product(s), the Data Processor shall either delete or return 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 this DPA.

C.5. Processing location

Processing of the personal data under the DPA cannot be performed at other locations than the following without the Data Controller’s prior written authorisation:

The Data Processor is located within Europe, and the processing can take place in the locations where the Data Processor and all entities within Karnov Group are located. A list of Group entities can be provided upon request.

Furthermore, Cloud solutions of Google (Google Cloud Platform) and Microsoft (Microsoft Azure) are used for hosting the Licensed Product(s) provided by the Data Processor. The supporting infrastructure is physically located in European datacentres in Ireland, Netherland and Sweden.

Physical access to servers is restricted to authorized personnel of Google and Microsoft.

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

If the data controller does not in the DPA 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 DPA to perform such transfer.

NAME	ADDRESS	DESCRIPTION OF PROCESSING	LEGAL BASIS FOR THE PROCESSING
Azure by Microsoft	Microsoft European data centers in the Netherlands & Ireland	Cloud hosting provider The data processor uses Microsoft Azure as a sub-processor. Data is stored on servers inside the EU and will generally **not** be transferred outside of the EU.	Standard Contractual DPA (SCC) and supplementary measures.
Azure OpenA AI by Microsoft	Microsoft European data center in Sweden	Generative AI service provider for functionality capabilities. The data processor uses Microsoft Azure as a sub-processor. Data is stored on servers inside the EU and will generally **not** be transferred outside of the EU.	Standard Contractual DPA (SCC) and supplementary measures.
Google Cloud Platform	Google European Datacentres in Germany & the Netherlands	Cloud hosting provider. The data processor uses Google Cloud Platform as a sub-processor. Data is stored on servers inside the EU and will generally **not** be transferred outside of the EU.	Standard Contractual DPA (SCC) and supplementary measures.
Google Vertex AI	Google European Datacentre in Germany	Generative AI service provider for functionality capabilities.	Standard Contractual DPA (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, obtain an annual audit statement from an independent third party concerning the data processor's compliance with the data protection regulation, data protection provisions of other EU or national law and these DPA.

The agreement between the parties is that the audit statement must be drafted in accordance with the ISAE 3000-framework or similar.

The audit statement can be sent to the data controller for information upon request.

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

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 used, as well as sub-sub-processors, etc.

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 these DPA.