GENERAL DATA PROTECTION POLICY

1. INTRODUCTION AND SCOPE

1.1 This is the data protection policy ("**Policy**") of Cognite AS ("**COMPANY**").

1.2 COMPANY is committed to protecting and respecting individual privacy. The specific purpose of this Policy is to ensure that COMPANY complies with EU data protection laws regulating the use of information concerning living individuals. In particular, COMPANY is from 25 May 2018, obliged to comply with the requirements and restrictions of the General Data Protection Regulation (EU) 2016/679 **(GDPR**).

1.3 This Policy regulates the "**Processing**" of "**Personal Data**". These terms are defined as follows:

1.3.1 **Personal Data** means information that:

(a) relates to an identified or identifiable living individual; and

(b) is held either (i) on computer or in other electronic or automatically Processable form; or (ii) in a paper filing system arranged to be accessible according to specified criteria.

1.3.2 **Processing** means collecting, storing, analysing, using, disclosing, archiving, deleting or doing absolutely anything else with Personal Data (and **Process**, **Processed** and **Processable** should be read accordingly).

1.4 COMPANY Processes Personal Data regarding individuals including its own employees and customers, individual representatives of its suppliers and other counterparties and business partners, including financial organisations (referred to in this Policy as **Data Subjects**), in the course of its business.

2. COMPLIANCE WITH THIS POLICY

2.1 All persons who Process Personal Data for or on behalf of COMPANY, including employees, must comply with this Policy. Failure to comply with this Policy is a serious matter which may give rise to disciplinary sanctions, up to and including dismissal.

2.2 COMPANY shall keep an appropriate record of COMPANY's Processing of Personal Data.

3. RESPONSIBLE DEPARTMENTS

The CEO is responsible for the administration of this Policy.

4. DESIGN AND ASSESSMENT OF PROCESSING ARRANGEMENTS

4.1 Where a new information technology system or other arrangement involving the Processing of Personal Data (a **Processing System**) is to be implemented within or on behalf of COMPANY, or a significant change is to be made to an existing Processing System, the new Processing System or change should be designed and assessed to ensure that full account is taken of the requirements of this Policy and the privacy of Data Subjects in the selection, design and implementation of the new elements of the new or changed Processing System, including in particular:

4.1.1 seeking to keep the Personal Data to be Processed by the Processing System to the minimum level consistent with COMPANY's business and other requirements;

4.1.2 where Personal Data are to be Processed and this is reasonably practicable and consistent with those requirements, keeping data allowing the identification of Data Subjects separate from other elements of the relevant Personal Data, and effectively protected, so that the Data Subjects are not identifiable except where this is Necessary for COMPANYs' business or other purposes; and

4.1.3 ensuring that the Processing of Personal Data carried out by the Processing System will comply with this Policy.

4.2 The requirements of section 4.1 are addressed through the change management process managed by the CEO. Any employee who is aware of a new Processing System, or a significant change to an existing Processing System, which may not have been referred to the relevant change management process, should consult the CEO.

4.3 Written records shall be kept of the assessments referred to in section 4.1 and that, if the assessment concludes that the new or changed Processing System will result in high risks for the privacy of the relevant Data Subjects, a data protection impact assessment should be conducted in accordance with article 35 of the GDPR.

5. TRANSPARENCY

5.1 In relation to each Processing System, COMPANY will establish and follow procedures to ensure that, except as provided in section 5.2, Data Subjects are provided with the information set out in the Annex to this Policy, if they do not already have it, before the Processing of their Personal Data begins (or, if later, as soon as practicable after this Policy takes effect). The information should be provided in writing, in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

5.2 Note the following points:

5.2.1 ***Employees*** are provided with and periodically reminded of information about the Processing of their Personal Data through COMPANY's internal employee handbooks (the **Employee Handbook**). Provision of this information does not need to be repeated through separate notices and communications, but employees should be provided with any information about each Processing System which is not included in the Employee Handbook.

5.2.2 COMPANY has a privacy notice published on its website, which makes available information about COMPANY's Processing of Personal Data to a wide range of other individuals, including visitors to its premises, visitors to its website, beneficial owners and other representatives of its suppliers, customers, regulators and other business partners. COMPANY takes the view that it is not necessary to provide each of these individuals directly with a full statement of the information set out in Annex 1, in relation to routine Processing of their Personal Data for business purposes, but where practicable their attention be drawn to the privacy statement.

5.2.3 Data Subjects need not be provided with information as otherwise required by section 5.2.1 in the following circumstances:

(a) if COMPANY is Processing the relevant Personal Data in order to investigate an alleged regulatory breach or disciplinary issue, and to provide the information would prejudice the investigation;

(b) if the relevant Personal Data are not obtained by COMPANY directly from the Data Subject but from a third party, and to contact and inform the Data Subject would be impossible, or would require effort disproportionate to the value to the Data Subject of being informed (but in those circumstances COMPANY will instead publish the information on its website); or

(c) otherwise, if the CEO has been consulted and COMPANY has concluded in writing that the GDPR and other applicable laws do not require the information to be provided.

6. FAIRNESS, LEGITIMACY AND PROPORTIONALITY

6.1 COMPANY will only Process Personal Data fairly and for specified and explicit purposes. These purposes are set out in the record of processing which is separately prepared and retained by COMPANY – if in doubt as to whether particular purposes are covered by this record, consult the CEO.

6.2 In particular, COMPANY will generally only Process Personal Data if:

6.2.1 the Processing is Necessary for the purposes of the legitimate interests that it, and the other persons with which it co-operates in the course of its business and wider operations, pursue (and by **Necessary** we mean that those purposes could not reasonably be achieved without the relevant Processing); and

6.2.2 either the Processing does not prejudice the privacy of the affected Data Subjects or, if there is some prejudice, it is sufficiently trivial or minor that it does not override the need to pursue those legitimate interests.

COMPANY will only Process Personal Data on this basis (the **Legitimate Interests Condition**) where it has considered the matter and concluded that the test in sections 6.2.1 and 6.2.2 is met.

6.3 Where the Legitimate Interests Condition does not apply, COMPANY will not Process Personal Data unless:

6.3.1 the Processing is Necessary so that COMPANY can perform a contract with the Data Subject or take steps at his or her request with a view to entering into such a contract;

6.3.2 the Processing is Necessary so that COMPANY can comply with its legal obligations;

6.3.3 the Data Subjects have Consented to the Processing of their Personal Data for one or more specified purposes;

6.3.4 the Processing is Necessary to protect the Data Subject's (or another person's) "vital interests" (where this is a matter of life or death); or

6.3.5 the CEO has been consulted and COMPANY has concluded in writing that the Processing is consistent with the requirements of the GDPR and other applicable laws.

6.4 COMPANY will not Process Personal Data which are irrelevant or inadequate or go beyond what is necessary given the purposes of the Processing.

6.5 Having collected Personal Data for a particular purpose, COMPANY will not then Process those Personal Data in a way which is incompatible with that purpose unless it first obtains the Data Subject's Consent.

7. SENSITIVE PERSONAL DATA

7.1 COMPANY will take particular care in relation to the Processing of Personal Data in the following, sensitive categories (**Sensitive Personal Data**):

7.1.1 Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;

7.1.2 genetic data and biometric data Processed for the purpose of uniquely identifying a living individual;

7.1.3 Personal Data concerning a living individual's health, sex life or sexual orientation; and

7.1.4 Personal Data relating to criminal convictions and offences or related security measures.

7.2 In particular, COMPANY will not Process Sensitive Personal Data except where:

7.2.1 the Data Subject has given his or her explicit Consent to the Processing for one or more specified purposes;

7.2.2 the Processing is Necessary for the purposes of performing obligations or exercising specific rights under employment and social security and social protection law;

7.2.3 the Processing is Necessary to protect the Data Subject's (or another person's) "vital interests" (where this is a matter of life or death) and the Data Subject is physically or legally incapable of giving Consent;

7.2.4 the Sensitive Personal Data has been deliberately made public by the Data Subject; or

7.2.5 the CEO has been consulted and COMPANY has concluded in writing that the Processing is consistent with the requirements of the GDPR and other applicable laws.

8. INTERNATIONAL DATA TRANSFER

8.1 COMPANY will only Transfer Personal Data outside the European Economic Area (the **European Region**):

8.1.1 where the Transfer is to a country or other territory which has been assessed by the European Commission as ensuring an adequate level of protection for Personal Data;

8.1.2 where the Data Subjects have given their explicit Consent to the Transfer taking place; or

8.1.3 where the Transfer is pre-approved by this Policy (see section 8.3 below), the CEO has been consulted and COMPANY has concluded in writing that the Transfer is compliant with the GDPR and other applicable laws.

8.2 For the purposes of this Policy, a **Transfer** is any transfer of Personal Data. This includes arrangements through which a person outside the European Region has remote access to Personal Data stored within the European Region.

8.3 COMPANY may prepare data transfer agreements (based on EU Model Clauses) which allows Personal Data to be Transferred between COMPANY and third parties. International Transfers can be made if they fall within the scope of those agreements, and the agreements can be amended so that it applies to new Transfers.

9. CONSENT

9.1 Personal Data can sometimes be Processed on the basis of Data Subject Consent (see sections 6.3 and 6.5 above). Sensitive Personal Data can sometimes be Processed, and Personal Data can sometimes be Transferred internationally, on the basis of explicit Data Subject Consent (see sections 7.2.1 and 8.1.2 above).

9.2 For the purposes of this Policy, **Consent** means a freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or a clear affirmative action (such as ticking a box), signifies agreement to the Processing of his or her Personal Data. Mere failure to respond does not amount to Consent.

9.3 Consent can be withdrawn at any time. COMPANY does not rely on Consent where Processing is not genuinely optional from the perspective of the Data Subject.

9.4 If COMPANY wishes to obtain the Consent (including the explicit Consent) of a Data Subject for the purposes of this Policy, it will:

9.4.1 request the Consent in an intelligible and easily accessible form, using clear and plain language;

9.4.2 make sure that the Data Subject understands, when he or she Consents, that he or she is free to withhold the requested Consent without suffering any adverse consequence, and that the Consent can be withdrawn at any time, with information as to a straightforward way in which the Data Subject can withdraw the Consent;

9.4.3 if the Consent is obtained in written form, and the relevant document also concerns other matters, make sure that the Consent is clearly distinguishable from the other matters; and

9.4.4 make sure that COMPANY has an appropriate record of the Consent having been given.

9.5 Where explicit Consent is required, COMPANY will need to explain in specific terms the nature of the Processing to be carried out and the Personal Data to be Processed, as well as providing all the information set out in Annex 1, and the Data Subject will then need to make an explicit written statement agreeing that the Processing can go ahead.

9.6 Where COMPANY has in place a Processing System involving the routine Processing or international Transfer of Personal Data, or any Processing of Sensitive Personal Data, based on Consent, it will ensure that the principles set out in section 9.4 are built into the arrangements for the implementation of that Processing System.

10. ACCURACY AND CURRENCY

Where COMPANY Processes Personal Data it will take every reasonable step to ensure that those Personal Data are accurate and, where relevant, up to date, and to correct inaccurate Personal Data without delay.

11. RETENTION AND DESTRUCTION

COMPANY will delete or anonymise Personal Data when they are no longer needed, in accordance with HR Norge's guidelines.

12. DATA SECURITY

12.1 COMPANY will have technical and organisational security measures in place to protect all Personal Data within each of its Processing Systems. These security measures must be appropriate to the risks of varying likelihood and severity for the rights and freedoms of individuals associated with the Processing of Personal Data within the relevant Processing System and, in particular, with the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to those Personal Data. In assessing what security measures are appropriate, COMPANY will take into account the state of the art (i.e. what security measures are available to be implemented), the costs of implementation and the nature, scope, context and purposes of the Processing to be carried out by the relevant Processing System. Where appropriate, they will include:

12.1.1 pseudonymisation and encryption of Personal Data;

12.1.2 the ability to ensure the ongoing confidentiality, integrity, availability and resilience of the Processing System;

12.1.3 the ability to restore the availability of, and access to, Personal Data in a timely manner in the event of a physical or technical incident; and

12.1.4 a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the Processing System.

12.2 Where COMPANY outsources the Processing of Personal Data to any third party service provider it will:

12.2.1 conduct appropriate due diligence on the technical and organisational security arrangements that the service provider will have in place to protect those Personal Data;

12.2.2 ensure that the arrangement is governed by a written agreement imposing obligations on the service provider as described in Annex 2 to this Policy; and

12.2.3 take reasonable steps (for example by exercising audit rights and/or making enquiries of the service provider) to ensure that the security measures required of the service provider are in place in practice over time during the life of the relevant Processing arrangement.

12.3 COMPANY is obliged to report certain breaches of security affecting Personal Data to competent data protection authorities witwhin 72 hours, and in some circumstances it is obliged to inform affected Data Subjects. An employee who becomes aware of or suspects such a breach must inform the CEO immediately so that COMPANY can comply with these obligations and, generally, investigate and respond to the apparent breach.

13. AUTOMATED DECISION-TAKING TECHNIQUES (INCLUDING PROFILING)

COMPANY will not use Processing Systems to take decisions producing legal effects concerning living individuals, or otherwise significantly affecting them, based solely on automated Processing of Personal Data, unless the CEO has been consulted in a particular case and COMPANY has concluded in writing that it meets the requirements of the GDPR and other applicable laws.

14. DATA SUBJECTS' RIGHTS

14.1 Data Subjects have the right:

14.1.1 to be provided with a copy of any Personal Data that COMPANY holds about them, with certain related information;

14.1.2 to require COMPANY, without undue delay, to update or correct any inaccurate Personal Data, or complete any incomplete Personal Data, concerning them;

14.1.3 to require COMPANY to stop processing their Personal Data for direct marketing Purposes; and

14.1.4 to object to the processing of their Personal Data more generally.

14.2 Data Subjects may also have the right, in certain circumstances:

14.2.1 to require COMPANY, without undue delay, to delete their Personal Data;

14.2.2 to "restrict" COMPANY's Processing of their Personal Data, so that it can only continue subject to very tight restrictions; and

14.2.3 to require Personal Data which they have provided to COMPANY, and which are Processed based on their Consent or the performance of a contract with them, to be "ported" to them or a replacement service provider.

14.3 If COMPANY receives a communication from any Data Subject in which he/she seeks to exercise any of these rights, that communication should be passed to the CEO as soon as is reasonably practicable so that COMPANY can respond appropriately.

15. CO-OPERATION WITH DATA PROTECTION AUTHORITIES

COMPANY will co-operate with competent data protection authorities in the performance of their tasks. Any communication received from a competent data protection authority should be passed to the CEO as soon as is reasonably practicable.

ANNEX 1
INFORMATION TO BE PROVIDED TO DATA SUBJECTS

The information referred to in section 5.1 of this Policy is:

1. COMPANY's identity and contact details;

2. if relevant, the contact details of COMPANY's data protection officer;

3. the purposes for which COMPANY intends to Process the Personal Data;

4. the legal basis for the Processing (e.g. the Legitimate Interests Condition);

5. where the Processing is justified on the basis of the Legitimate Interests Condition, the relevant legitimate interests pursued by COMPANY;

6. where COMPANY is not collecting the Personal Data directly from the Data Subject but from a third party, the categories of Personal Data collected and the sources from which they are collected (including, if relevant, the fact that Personal Data are obtained from publicly available sources);

7. any intended recipients or categories of recipient of the Personal Data (this means recipients outside COMPANY, such as third party service providers);

8. where applicable (see also section 8), the fact that COMPANY intends to Transfer the Personal Data to a country or territory outside the European Region, together with information as to:

    8.1.1 whether the relevant country has been determined by the European Commission to ensure an adequate level of protection for Personal Data; and

    8.2 where this is not the case, and if COMPANY justifies Transferring the Personal Data to that country or territory on the basis that it has put in place adequate safeguards to protect the Transferred Personal Data, the nature of those safeguards and details of a contact point from whom a copy of the relevant safeguards can be obtained;

9. the period for which the Personal Data will be stored, or if that is not possible, the criteria used to determine that period (see also section 11);

10. the existence of the legal right to request from COMPANY access to and rectification or erasure of Personal Data or restriction of Processing concerning the Data Subjects or to object to Processing as well as the right to data portability (see also section 14), and that these rights can be exercised by contacting the CEO;

11. that the Data Subjects can, if they so wish, lodge a complaint about COMPANY's Processing of his or her Personal Data with the relevant national data protection authority;

12. where COMPANY is collecting the Personal Data directly from the Data Subjects, whether provision of the requested Personal Data is a statutory or contractual requirement, or a requirement Necessary to enter into a contract, and whether the Data Subject is obliged to provide the Personal Data and the possible consequences of failure to provide it; and

13. detailed information about any automated decision-taking techniques that may be used (see section 13).

ANNEX 2
PROVISIONS TO BE INCLUDED IN DATA PROCESSING AGREEMENTS

1. The agreement should set out the subject matter of the Processing to be carried out by the service provider, its duration, the nature and purpose of the processing, the types of Personal Data to be Processed by the service provider, the categories of Data Subjects and COMPANY's obligations and rights.

2. The agreement should require that the service provider:

   2.1 processes the Personal Data only on documented instructions from COMPANY, including with regard to Transfers of Personal Data outside the European Region, unless required to do so by EU/EEA member state (or, where relevant, Norwegian) law to which the service provider is subject (in such a case, the service provider should be obliged to inform COMPANY of that legal requirement before Processing, unless that law prohibits providing such information on important grounds of public interest);

   2.2 ensures that persons authorised to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

   2.3 takes all the data security measures required pursuant to the GDPR (even if it is not itself directly subject to the GDPR);

   2.4 does not appoint a person to Process the Personal Data on its behalf except with the prior consent of COMPANY, and (in the case of a general consent) gives COMPANY an opportunity to object to any changes in its sub-processing arrangements;

   2.5 taking into account the nature of the Processing, assists COMPANY by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of COMPANY' obligation to respond to requests for exercising the Data Subject's rights laid down in chapter III of the GDPR (see section 14);

   2.6 assists COMPANY in ensuring compliance with its data security, security breach notification, impact assessment and data protection authority consultation obligations under the GDPR, taking into account the nature of processing and the information available to the processor;

   2.7 at the choice of COMPANY, deletes or returns all the Personal Data to COMPANY after the end of the provision of services relating to Processing, and deletes existing copies, unless EU or EU member state (or, where relevant, Norwegian) law requires storage of the Personal Data;

   2.8 makes available to COMPANY all information necessary to demonstrate compliance with the obligations requires as set out above and allows for and contributes to audits, including inspections, conducted by COMPANY or an auditor mandated by COMPANY; and

   2.9 immediately informs COMPANY if, in its opinion, an instruction given by COMPANY (see 2.1 above) infringes the GDPR or any other law of the European Region.