LINDSKOG MALMSTRÖM ADVOKATBYRÅ'S PERSONAL DATA PROCESSING POLICY

1 Background and intention

1.1 Lindskog Malmström Advokatbyrå ("LMA") safeguards the integrity of its clients, partners and employees and always takes care to comply with the current data protection regulations. Everyone has a right to protection of the personal data concerning him or her.

1.2 LMA has therefore adopted this Policy for processing personal data to ensure that all those in the organisation comply with the data protection regulations. This document is intended to provide staff with detailed guidance on how to process personal data.

1.3 The General Data Protection Regulation came into force on 25 May 2018. It reinforces the protection for the individuals whose personal data is being processed and places more and stricter demands on organisations processing personal data.

1.4 If processing of personal data takes place in breach of the provisions of the General Data Protection Regulation, there is a risk of breaches in the personal integrity of the data subject but also a reputational risk for LMA. Furthermore, LMA may be liable to pay damages or be charged an administrative fine of up to twenty million euro or 4 % of the total global annual turnover, whichever is the higher amount. All staff are obliged to comply with these guidelines to avoid such consequences.

2 Area of application and scope

2.1 The policy applies to all LMA's employees and consultants in all markets and at all times.

2.2 LMA's partners shall ensure compliance with this Policy including training for all employees. Information to the employees shall also include information that breach of the policy may lead, for example, to consequences under labour law.

3 Basic principles

3.1 The basic principles described below shall always be complied with when processing personal data. LMA is responsible for and shall be able to show that the principles have been complied with.

3.2 Lawfulness, fairness, transparency – Personal data shall be processed in a lawful, correct and transparent way in relation to the data subject. Every type of processing shall have a legal basis, for example, contract performance, complying with a legal obligation, performing a public task, a legitimate interest

or consent (see section 5 below). If it is not possible to identify any legal basis applicable to the processing, the processing may not take place. Of fundamental importance for this principle is clear communication with the data subject on, among other things, the purposes for which personal data is processed, the type of processing that takes place, whether and how personal data is shared with others, and how to contact LMA. The data subject shall always be provided with clear and transparent information on the processing of their personal data.

3.3 Limitation of purpose – Personal data may only be collected and processed for special, explicitly stated and legitimate purposes and the data may not be subsequently processed in a way that is incompatible with these purposes.

3.4 Data minimisation – Personal data which is to be processed shall be adequate, relevant and not excessively extensive in relation to the purpose. Ensure that the data collected is actually needed and do not request data simply because it may be useful to have.

3.5 Accuracy – personal data that is processed shall be accurate and, if necessary, updated. Take suitable measures to ensure that incorrect or incomplete information is erased, for example, routines for changes of address when moving with a compilation of systems and registers where addresses are stored. Avoid, however, storing copies of information in many systems in order to avoid sources of error and saving incorrect information.

3.6 Storage limitation – Personal data may not be stored for a longer time than necessary taking into consideration the purposes of the processing. When data is no longer required, it must be culled, which means that it must either be erased or made pseudonymised.

3.7 The principle of accountability means that LMA must be able to show that it complies with the General Data Protection Regulation. LMA must therefore, for example, be able to document implemented and planned processes and measures that concern data protection issues.

3.8 Furthermore, there shall be a register of all types of processing of personal data performed and LMA must be able to show this register to the supervisory authority when so required.

4 Personal data

4.1 Personal data is all data that relates to an identified or identiable natural individual and which can directly or indirectly identify an individual. Examples of personal data are names, contact details, information about locality or factors specific for a person’s physical, economic, cultural or social identity. Data which may not be itself be subject to the requirements may still constitute personal data in combination with other data.

4.2 All processing of personal data is subject to the General Data Protection Regulation and its rules. Processing means a measure or combination of

measures relating to personal data, which is performed partly or wholly automatically. It also includes personal data in emails and in documents on servers, in a simple list, on websites and in other unstructured material.

4.3 Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership and the processing of genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation (special category data) is as a main rule prohibited. A valid exemption from the prohibition is required to permit such processing. The most common exemptions are the consent of the data subject or that the data subject has disclosed the data himself or herself, to exercise rights in the field of employment law, to be able to establish, exercise or defend legal claims or for health and medical care purposes.

4.4 Processing of personal ID numbers may only take place if it is clearly justified taking into consideration the purpose of the processing, the importance of secure identification or some other reason worthy of consideration.

4.5 Processing of data on convictions in criminal cases and offences or related security measures but probably not data on suspected crimes) may only be processed in certain special cases. As a law firm, we may process personal data if (i) the processing is necessary for checking that a conflict of interest does not exist, (ii) particular data necessary for establishing legal claims, or defence in a particular case or (iii) for control of money laundering.

5 Statutory basis for personal data processing

5.1 Personal data processing is only lawful if and to the extent that any of the following bases is applicable.

5.2 The data subject has given consent to personal data being processed for a particular purpose or purposes. Special requirements must be complied with for the consent to be valid.

5.3 Processing is necessary to perform a contract to which the data subject is a party or to undertake measures at the request of the data subject prior to such contract being entered into.

5.4 Processing is necessary to perform a legal obligation which LMA is subject to. An example which may be mentioned here is statements of tax paid and income submitted to the Tax Agency.

5.5 Processing is necessary to protect the vital interests of the data subject or another natural person (for example, when a danger to life is involved).

5.6 Processing is necessary to perform a task in the public interest (for example, as public defence counsel) or as part of the exercise of authority (for example, as a Public Notary).

5.7 Processing is necessary for the purposes of the legitimate interests pursued by

LMA or by a third party except where such interests are overriden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data (balancing of interests).There are special requirements on documentation for the assessment made in the case of balancing of interests.

6 Security measures, authorisation control and access, erasure

6.1 Personal data shall be processed in a way that ensures appropriate security for the personal data using technical and organisational measures. Organisational security measures may entail the use of authorisation control for the systems containing personal data, logging of access to personal data or that computers and similar containing personal data are to be located in such a way as to make unauthorised access difficult and not to be in an exposed position. Examples of technical measures that must be checked are if LMA has sufficient back-up routines, sufficient firewalls, password-protected wireless networks, updated virus protection, password protection for mobile units such as mobile telephones and tablets, protection against unauthorised internal access, password requirements, encryption when necessary, logging off, access to and use of IT systems, etc.

6.2 Personal data may not be kept for a long time than necessary taking into consideration the purpose of processing. Structured culling is ensured by establishing and complying with a culling routine for the respective database/processing. Personal data in so-called unstructured material such as documents on servers, in a simple list, on websites, etc. need to be erased when the purpose of processing has been complied with.

7 Transfer to a third country

Special rules apply for transfer of personal data to countries outside of the EU and EEA (third country transfer). The General Data Protection Regulation entails that all EU Member States and EEA countries have a similar protection for personal data and personal integrity and personal data can therefore be freely transferred within this area without restriction. There are, however, no general rules in countries outside the area providing corresponding guarantees and third-country transfer is therefore subject to special conditions. This affects every form of cross-border transfer of information, for example, many online IT services, cloud-based services, services for external access or global databases, etc., which need to be subject to a separate analysis.

8 Impact assessment

8.1 LMA has adopted a special routine to be able to identify and handle special risks to integrity in its activities and for structured follow-up. Special risks for the rights and freedoms of natural individuals may, for example, exist in connection

with a particular type of processing, especially sensitive data, processing to an especially large extent, use of new technology or similar.

8.2 If it is probable that new or changed personal data processing may in some particular aspect entail a high risk for the rights and freedoms of natural persons, the routine shall be complied with and an assessment made of the intended processing before starting processing.

8.3 Before starting such personal data processing, the management group shall be contacted to investigate whether an impact assessment is required and when necessary to perform the impact assessment with the responsible person.

9 Excerpts from registers and disclosure

9.1 The General Data Protection Regulation confers a number of rights on the data subjects as regards processing personal data. It is LMA's task to comply with these rights and ensure that there are sufficient processes to meet the wishes of data subjects.

9.2 The data subject has a right to information when personal data is collected. This information shall be kept in an easily accessible written form in easily comprehensible language. There are a number of clear requirements in the General Data Protection Regulation which must be complied with and the requirements vary depending on the information gathered from the data subject or from a third party.

9.3 The data subject has the right to be informed as to whether personal data belonging to the subject is being processed, and in such cases receive a copy of the personal data (register extract). This right applies regardless of the place where the personal data is processed.

9.4 If personal data being processed is inaccurate or incomplete, the data subject may request that it be corrected. If the data subject shows that the purpose for which the personal data is being processed is no longer permitted, necessary or reasonable in the circumstances, the personal data in question shall be erased, unless there are statutory provisions that provide otherwise.

9.5 The data subject has a right to transfer personal data which the data subject has submitted to LMA to another controller (right to data portability) if the processing is supported on the legal grounds of contract or consent. The personal data shall be provided to the data subject in a structured, generally used and machine-readable format. If it is technically possible, the data subject may request that the data is transferred directly to another controller. This right only applies to the personal data which the data subject has supplied to LMA himself or herself.

9.6 The data subject has in certain cases the right to demand that LMA restrict processing of his or her personal data, i.e. restrict processing to particular defined purposes. The right to restriction applies, inter alia, when the data

subject considers that the data is not accurate and has requested that it be rectified. The data subject may then request that processing of personal data is restricted during the period that the accuracy of the data is investigated. When the restriction ceases, the data subject will be informed to that effect.

9.7 The data subject has the right to object against processing of personal data which is supported on legitimate interest as a legal basis. In the event of an objection, LMA shall cease processing unless it can show that there exist mandatory legitimate grounds that weigh more heavily than the interests, rights and freedoms of the data subject or if the processing of personal data is performed for establishment, exercise or defence of legal claims.

9.8 In certain cases, the data subject has the right to request erasure of his or her personal data ("the right to be forgotten"). An example is when consent is the legal ground for processing and the data subject revokes his or her consent.

9.9 When personal data is processed for direct marketing, the data subject has at any time the right to object to processing of personal data about him or her. If a data subject opposes processing of personal data for direct marketing purposes, processing for such purposes shall cease.

10 Bankruptcy administration

10.1 LMA has lawyers who undertake work as bankruptcy administrators and who in this activity comply with the regulations on processing personal data. The bankruptcy administrator distinguishes processing of personal data which takes place within the framework of the bankruptcy administration and processing which is part of LMA's normal activities. This means that there may be two different data controllers in bankruptcy cases.

10.2 LMA is data controller for personal data which the bankruptcy administrator processes in its role as administrator, i.e. within the framework of LMA's normal activities as a law firm. LMA is responsible for such processing taking place in accordance with current regulations.

10.3 In bankruptcy cases, LMA obtains and processes personal data in order to perform the task assigned to as bankruptcy administrator at LMA. This processing is necessary to perform a public task or as part of the exercise of public authority that dealing with bankruptcy cases may entail (for example, decisions concerning salary guarantees for employees in a bankrupt company). LMA refers to other parts of this policy for other personal data processing in bankruptcy.

10.4 The bankruptcy estate is the data controller of personal data that the bankruptcy administrator processes within the framework of the activities of the bankruptcy estate and in the capacity of representative for the bankruptcy estate. The bankruptcy estate is responsible for such processing taking place in compliance with current regulations.

10.5 In order to enter into, deal with and perform contracts with you as creditor, debtor, supplier, auditor or accounting consultant employee or bank, the bankruptcy estate obtains personal data about you. The legal basis for the bankruptcy estate processing of your personal data is that it is necessary to perform the bankruptcy estate agreement with you or to undertake measures prior to such agreement being entered into. If you do not provide the above-mentioned personal data, the bankruptcy estate cannot perform its undertakings to you.

10.6 Personal data may be processed on the basis of the bankruptcy estate having a legal obligation to comply with, for example, personal data due to the bankruptcy estate's obligation to keep accounts or other obligations that rest on the bankruptcy estate by law.

10.7 In order to perform the task of bankruptcy administrator and to ensure that the bankruptcy estate is administered correctly and in accordance with the assignment given to the bankruptcy administrator, personal data may be processed on the basis that the processing is necessary to perform a task in the public interest. For example, it rests on the bankruptcy administrator, as representative of the bankruptcy estate, to ensure that creditors of the bankruptcy estate are not disadvantaged and that distribution of any assets takes place in an exemplary way.

10.8 The bankruptcy estate never stores data longer than necessary taking into consideration the purpose of the processing. The bankruptcy estate therefore carry out regular culling of stored personal data and remove the data that is no longer needed.

10.9 The bankruptcy estate will need to store personal data for a longer period, inter alia, to administer any guarantees, complaint deadlines, to comply with legal requirements, decisions by public authorities and to deal with legal claims that may be directed at the bankrupt company and the bankrupt estate. The bankruptcy estate may store personal data for up to 10 years in accordance with the Swedish Bar Association's guidelines.

10.10 Your personal data may be submitted to and processed by a third party. This may be a company, supplier of services, other legal advisors, auditors, consultants, public authorities etc. Examples of situations when your personal data may be transferred to a third party are when such a measure is required due to a law, dispute, enquiry or decision by a public authority, at your own request or when it is required to comply with the legitimate interests of the bankruptcy estate. The bankruptcy estate remains the controller for the personal data transferred, while the third party depending on circumstances will either become an independent controller, a joint controller with the bankruptcy estate or the bankruptcy estate's processor.

10.11 The provisions of sections 9 and 11 also, with due changes, apply in the situation where the bankruptcy estate is the controller.

10.12 In the event of questions or other requests concerning personal data in bankruptcies, see section 13 for contact information.

11 Personal data breaches

11.1 A personal data breach is a security breach leading to unintentional or unlawful destruction, loss, alteration or unauthorised access to personal data. Examples of personal data breaches might be theft of customer registers, unintentional disclosure of wage information via email to the wrong recipient, an employee taking home a non-encrypted work computer which is subsequently stolen in a break-in and which leads to information about employees or customers being disclosed, personal data which is published on the web by mistake, a laptop containing personal data which is lost or stolen, etc.

11.2 Personal data breaches may need to be notified to the supervisory authority within 72 hours of detection of the breach if it is probable that there is a risk to the rights and freedoms of natural persons. Breaches that occur shall be documented and it may be necessary to notify the data subjects concerned.

11.3 In the event of a suspected personal data breach, contact the management group immediately on +46 (0)8 599 290 00 or at info@lmlaw.se. The management group will then determine whether it is necessary to contact the supervisory authority or the data subject.

12 Miscellaneous

12.1 See the General Data Protection Regulation for definitions of the terms used in this policy.

12.2 The Swedish Bar Association has drawn up a guideline for application of the EU General Data Protection Regulation in lawyer's activities, which is referred to for further information.

12.3 This policy shall be updated as necessary.

13 Further information

In the event of questions pertaining to processing of personal data, please contact the management group on +46(0)8-599 290 00 or info@lmlaw.se.

Policy adopted by LMA's management group on 30 October 2019.