LANDAHL ADVOKATBYRÅ'S PERSONAL DATA PROCESSING POLICY

---

1 Background and purpose

1.1 Landahl Advokatbyrå safeguards the privacy of its clients, partners, and employees and is careful at all times to comply with applicable data protection regulations. Every individual is entitled to the protection of any and all personal data that concerns him or her.

1.2 Landahl Advokatbyrå has accordingly adopted this Policy for the processing of personal data in order to ensure that everyone within the organisation complies with the data protection rules. This document is designed to give you, as an employee, more detailed guidance on how you should process personal data.

1.3 The General Data Protection Regulation (GDPR) came into force on 25 May 2018. It entails stronger protection for those persons whose personal data is processed and imposes additional and stricter requirements on organisations processing personal data.

1.4 If the processing of personal data would entail a contravention of the provisions of the GDPR, the risk exists not only of the personal privacy of the data subject being infringed, but also of the reputation of Landahl Advokatbyrå being damaged. The firm may, furthermore, be obliged to pay damages or have an administrative penalty fee imposed of up to EUR 20 million or 4% of global turnover, whichever is the greater. All employees are obliged to comply with these guidelines in order to avoid such consequences.

2 Ambit and scope

2.1 The policy applies to all Landahl Advokatbyrå employees and consultants, in all markets and at all times.

2.2 The Board of Directors of Landahl Advokatbyrå shall ensure compliance with this Policy, including by means of the provision of training for all employees. The information provided for employees shall also include information stating that breaches of the policy may have, amongst other things, employment law consequences.

2.3 Routines and forms have been developed for certain sections and shall be used as necessary. Employees will find links to these routines and forms for the issue in question under G:/Therefore under GDPR.

3 Fundamental principles

3.1 The fundamental principles described below shall be observed at all times when processing personal data. Landahl Advokatbyrå is responsible for and shall be able to demonstrate compliance with the principles.

3.1.1 *Lawfulness, fairness, transparency* – Personal data shall be processed in a manner that is lawful, correct, and transparent in relation to the subject. Every type of processing shall,

therefore, be based on so-called lawful grounds, such as the fulfilment of an agreement, the fulfilment of a legal obligation, performing a task in the public interest, legitimate interest, or consent (see section 5 below). If no lawful grounds applicable to the processing can be identified, the processing may not, therefore, be performed. The starting point for this principle is clear communication with the data subject with regard to, amongst other things, the reason for which the personal data is being processed, the type of processing that will be performed, whether and in what way the personal data is shared with others, for how long the personal data is stored, and how to contact Landahl Advokatbyrå. The data subject shall, in other words, be provided with clear and transparent information on the processing of their personal data.

3.1.2 *Purpose limitation* – Personal data may only be collected and otherwise processed for specific, explicitly stated, and justifiable purposes and may not subsequently be processed in a way that is incompatible with these purposes.

3.1.3 *Data minimisation* – Personal data that is processed shall be adequate, relevant and not overly extensive in relation to the purposes. Make sure that the data collected is genuinely required and do not ask for information simply because it might be useful to have.

3.1.4 *Accuracy* – Personal data processed must be accurate and, if necessary, updated. Put appropriate measures in place to ensure that incorrect or incomplete data is corrected, e.g. change of address routines in conjunction with relocation with a compilation of systems and registers where the address is stored. You should, however, avoid storing copies of data in multiple systems in order to avoid source errors and storage of non-updated information.

3.1.5 *Storage limitation* – Personal data may not be retained for longer than it is needed for the purpose of the processing. When the data is no longer needed, it must be weeded, i.e. it must be either erased or anonymised.

3.1.6 *Privacy and confidentiality* – Personal data must be protected against, amongst other things, unauthorised or prohibited access and against accidental loss, destruction, or damage. Landahl Advokatbyrå must, therefore, implement appropriate technical and organisational measures to protect the personal data.

3.1.7 *Security* – Landahl Advokatbyrå shall ensure that the personal data is protected in a way that is appropriate with regard to the protection value of the personal data and the risk of it being abused. Sensitive personal data requires a higher level of protection than other data.

3.1.8 *Privacy by design or privacy by default* – Privacy by design means that consideration must be given to GDPR when building IT systems and formulating work routines. Privacy by default means, in brief, that the person processing the personal data shall ensure that the personal data is not, by default, processed unnecessarily.

3.1.9 *Accountability* – The accountability principle means that Landahl Advokatbyrå must be able to demonstrate compliance with GDPR. The agency must, therefore, be able to document implemented and planned processes and measures in relation to data protection issues, for example.

A register of all types of personal data processing performed shall also be maintained and Landahl Advokatbyrå shall be able to submit a register of this kind to the supervisory authority when required.

4 Personal data

4.1 *Personal data* refers to all data that refers to an identified or identifiable natural person and which can, either directly or indirectly, identify a person. Examples of personal data include their name, contact details, localisation data, or factors that are specific to a person's physical, economic, cultural, or social identity. Data which does not individually meet these criteria may nonetheless comprise personal data when combined with other data.

4.2 All personal data processing is subject to GDPR and its provisions. The term, *processing*, refers to a measure or combination of measures in relation to personal data which is carried out either wholly or partially automatically. The definition also applies to personal data in emails and documents on servers, in a simple list, on websites, and in other unstructured material.

4.3 Processing of personal data that reveals race or ethnic origin, political opinions, religious or philosophical beliefs, or membership of trade unions, together with processing of genetic data, biometric data, health data, or data concerning a person's sex life or sexual orientation (so-called *special categories of personal data*) is, as a general principle, prohibited. A valid exemption from this prohibition is required for such processing. The most common exemptions are when the data subject has granted consent or personally published the information, in order to exercise rights or fulfil obligations under labour law, in order to establish, cite, or defend legal claims, or for health and medical purposes.

4.4 *National identity number* processing may only occur when it is clearly motivated with regard to the purpose of the processing, the importance of reliable identification, or some other admissible reason.

4.5 Processing of personal data relating to *criminal convictions and offences* (convictions in criminal cases and breaches or associated security measures but probably not data on suspected offences) may only be processed in certain specific cases. As a law firm, we may process personal data if (i) the processing is necessary in checking that no conflict of interest exists, (ii) individual data that is necessary in establishing, citing, or defending a legal claim in a specific case, provided that the Swedish Authority for Privacy Protection has issued a ruling on this matter, or (iii) for purposes of money-laundering checks.

5 Lawful grounds for processing personal data

5.1 Processing of personal data is only lawful if and to the extent that any one of the following grounds apply.

5.1.1 The data subject has given their *consent* to the processing of the personal data for one or more specific purposes. Specific requirements exist that must be met for the consent to be valid.

5.1.2 The processing is necessary for the *performance of a contract* to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

5.1.3 The processing is necessary for *compliance with a legal obligation* to which Landahl Advokatbyrå is subject, such as control data submitted to the Swedish Tax Agency.

5.1.4 The processing is necessary in order to protect the *vital interests* of the data subject or another natural person (e.g. with regard to life-threatening danger).

5.1.5 The processing is necessary for the performance of a *task in the public interest* (e.g. as a public defender) or in the exercise of official authority (e.g. as a Notary Public).

5.1.6 The processing is necessary for purposes relating to the legitimate interests of Landahl Advokatbyrå or a third party, except where such interests are outweighed by the interests or fundamental rights and freedoms of the data subject which require protection of personal data (*weighing of interests*). Special requirements exist for documentation of the assessment performed in connection with the weighing of interests.

6 Security measures, permissions control and access, deletion

6.1 Personal data shall be processed in a way that ensures adequate security for the personal data through the use of technical and organisational measures. Organisational security measures may entail the use of permissions controls for the systems that hold personal data, logging of access to personal data, or computers et al that hold personal data are stored so as to prevent unauthorised access and that are not left accessible. Examples of technical measures that must be checked include whether Landahl Advokatbyrå has adequate backup routines, adequate firewalls, password-protected wireless networks, updated virus protection, password protection for mobile devices such as mobile phones and tablets, protection against unauthorised internal access, password requirements, encryption where necessary, logging off, access to and use of IT systems, etc.

6.2 Personal data may not be stored for longer than is necessary with regard to the purpose of the processing. Drawing up and following a weeding routine for each database/processing ensures structured weeding work. Personal data in what is known as unstructured material, such as documents on servers, in a simple list, on websites, etc., must also be deleted when the purpose of the processing has been achieved.

7 Transfers to third countries

7.1 Special rules apply to the transfer of personal data to countries outside the EU or EEA (known as third country transfers). The GDPR means that all EU member states, and EEA countries have equivalent protection for personal data and personal privacy, and personal data can, therefore, be freely transferred within the area with no restrictions. There are, however, no general rules offering equivalent guarantees for countries outside the area and third country transfers are, therefore, only permitted under special circumstances. This applies to every form of cross-border transfer of information, e.g. many online IT services,

cloud-based services, external access services, or global databases, etc., and special analysis is, therefore, required.

8 Impact assessment

8.1 Landahl Advokatbyrå has a special routine in place enabling it to identify and manage special privacy risks within the operations and for structured follow-up purposes. Special risks to the rights and freedoms of natural persons may, for example, arise in conjunction with a particular type of data processing, particularly sensitive data, processing on a particularly large scale, the use of new technology, etc.

8.2 If a new or amended type of personal data processing could, in a specific respect, probably entail a high risk to the rights and freedoms of natural persons, the routine shall be followed and an assessment of impacts of the intended processing on the protection of personal data shall be conducted before the processing begins.

8.3 Before any such personal data processing begins, the HR Manager (firstly) and a Member of the Board (secondly) shall be contacted in order to determine whether an impact assessment is required and any impact assessment deemed necessary shall then be performed in cooperation with the person responsible for the processing by answering certain specific questions, through work meetings, and through risk assessment.

9 Register extracts and disclosure

9.1 The GDPR gives data subjects a number of rights with regard to the processing of personal data. Landahl Advokatbyrå is obliged to comply with these rights and to ensure that adequate processes are in place to enable the law firm to act on a data subject's request in relation thereto.

9.1.1 The data subject is entitled to *information* when personal data is collected. This information shall be provided in an easily accessible written form, using clear and plan language. The GDPR mandates a number of clear requirements that must be met, and these requirements vary, depending on whether the information has been collected from the data subject themselves or from a third party.

9.1.2 The data subject is entitled to confirmation of whether personal data belonging to the subject is being processed, and where that is the case, to obtain a copy of the personal data (*register extract*). This right applies irrespective of the location in which the personal data is being processed.

9.1.3 If personal data being processed is incorrect or incomplete, the data subject may demand *rectification*. If the data subject can show that the purpose for which the personal data is being processed is no longer permitted, necessary, or reasonable under the circumstances, the personal data in question shall be *deleted* in the absence of any legal provisions to the contrary.

9.1.4 The data subject has the right to transfer personal data they have provided to Landahl Advokatbyrå to another controller (*right to data portability*) if the processing is supported by

the legal grounds' agreement or consent. Personal data shall be provided to the data subject in a structured, commonly used and machine-readable format. The data subject shall, where technically feasible, have the right to demand that the data be transferred directly to another controller. This right only applies to the personal data that the data subject has, themselves, submitted to Landahl Advokatbyrå.

9.1.5 The data subject has, in certain cases, the right to demand that Landahl Advokatbyrå *restrict the processing* of their personal data, i.e. restricts the processing to certain delimited purposes. The right to restriction applies when amongst other things, the data subject holds that the data is incorrect and has requested rectification of the personal data. The data subject can then demand that the processing of personal data be restricted while the accuracy of the personal data is investigated. The individual shall be notified when the restriction is lifted.

9.1.6 The data subject has the right to *object to the processing* of personal data with legitimate interest as the lawful grounds. When an objection is submitted, the law firm shall cease processing of the data unless it is able to demonstrate compelling legitimate grounds for the processing which outweigh the interests, rights, and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

9.1.7 The data subject has, in certain cases, the right to demand the erasure of their personal data ("*the right to be forgotten*"). One example of this may be when consent is the legal ground for the processing and the data subject withdraws their consent.

9.1.8 When personal data is processed for *direct marketing purposes*, the data subject has the right to object at any time to the processing of personal data concerning them. If a data subject objects to the processing of personal data for direct marketing purposes, the processing for such purposes shall cease.

10 Personal data breaches

10.1 A personal data breach is a security breach that leads to the unintentional or illegal destruction, loss, alteration of, or unauthorised access to personal data. Examples of personal data breaches may involve the theft of client lists, unintentional disclosure of salary information via emails to the wrong recipient, an employee taking an unencrypted work computer home with them that is then stolen during a burglary and which leads to the disclosure of information on employees or clients, personal data being published online by mistake, a laptop containing personal data being lost or stolen, etc.

10.2 Personal data breaches may need to be reported to the supervisory authority within 72 hours of the breach being detected if it is likely that a risk to the rights and freedoms of natural persons exist. Breaches that occur shall be documented and it may be necessary to notify affected data subjects.

10.3 When a personal data breach is suspected, you should first contact the HR Manager and then a Member of the Board, as per the internal contact list. The Board will then determine whether the supervisory authority or the data subject must be notified.

11 Other

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

11.2 The Swedish Bar Association has drawn up guidelines for the implementation of the EU's General Data Protection Regulation in the context of law firms' operations. These guidelines are available on the Swedish Bar Association's website, to which reference is made for further information.

11.3 This policy shall be updated annually or as needed on the basis of instructions from, firstly, the HR Manager, and secondly, a Member of the Board.

12 Questions

If you have any questions regarding the processing of personal data, please contact, first, the HR Manager, and secondly, a Member of the Board.

Policy adopted by the Board of Directors of Landahl Advokatbyrå on 16 May 2018