Van Lanschot Kempen

Compliance Requirements Document

—

Privacy and protection of personal data

Area of application
The principles stated in this document apply to all staff at Van Lanschot Kempen in the Netherlands and elsewhere. Van Lanschot Switzerland has a comparable regulation aligned with its own organisation and taking into account local legislation and regulation where they apply

Issued by
Compliance
Contactperson Kurt Aulman, Privacy Officer Van Lanschot Kempen

Date
January 2019

Version
January 2019

Introduction

1.1 Goal and guiding principles

Van Lanschot Kempen's business operations involve the processing of personal data. This data contains information about a natural person for the purpose of verifying someone's identity in a reasonable fashion, without excessive effort. This information includes the name of the person concerned, as well as their address, telephone number, date of birth, civil registration/social security number ("BSN" in Dutch), e-mail address, IP address, photos, videos, internet use and personal interests, as well as financial information.
Van Lanschot Kempen processes personal data of clients, prospective clients (hereinafter: prospects), persons linked to clients, contacts of business relations, its own staff members and job applicants – hereinafter: the party or parties concerned. The individuals in all these categories should be able to trust that the personal data they provide to Van Lanschot Kempen is handled securely and with integrity, and that Van Lanschot Kempen is transparent in this respect.

This requirements document describes the principles to be observed by staff at Van Lanschot Kempen when processing personal data of **clients, prospects, persons linked to clients, and contacts of business relations**. Processing of personal data refers to every type of action involving personal data, from collecting to deleting personal data (e.g. recording, storing, processing, handing over, distributing, collecting, etc.).
The principles described in this document also concern the processing of the personal data of **Van Lanschot Kempen staff and job applicants**.

Van Lanschot Kempen is bound by the General Data Protection Regulation (hereinafter: GDPR), local legislation on the implementation of the GDPR and local legislation on the implementation of the ePrivacy Directive[1]. In addition, there are the Guidelines and Opinions of the Working Party 29 (hereinafter: WP29), the current European Data Protection Board (hereinafter: EDPB), which provide further details for one or more articles or topics in the GDPR.
The principles stated in this requirements document are a translation from this legislation and regulations to the situation at Van Lanschot Kempen.

1.2 Area of application

The principles stated in this document apply to all staff at Van Lanschot Kempen

[1] The ePrivacy Directive will be replaced by the ePrivacy Regulation in early 2019.

in the Netherlands and elsewhere. Van Lanschot Switzerland has a comparable regulation aligned with its own organisation and taking into account local legislation and regulation where they apply.

2. General principles

Transparancy and accountability require Van Lanschot Kempen to observe the following principles when processing personal data:

- *Personal data is collected for well-defined, explicitly described and justified purposes*

  In the case of a financial institution such as Van Lanschot Kempen, the purposes of personal data collection predominantly concern activities such as:

  - Assessing and accepting relations and resulting activities such as entering into contracts, providing advisory and management services, and executing payment transactions;
  - Marketing activities aimed at maintaining or expanding existing client relationships or attracting new clients;
  - Risk management such as combating, preventing and identifying actions directed against Van Lanschot Kempen or the financial sector as a whole;
  - Meeting legal obligations (such as Client Due Diligence, determining risk profiles concerning securities investment advice, and asset management).

- *There have to be lawfull grounds for processing personal data*

  A financial institution such as Van Lanschot Kempen can, in general, collect and process personal data for any of the following lawfull grounds:

  - The personal data is typically needed for honouring a contract or for carrying out necessary actions prior to entering into a contract (e.g. application for opening an account, request for a quote for a mortgage loan, agreeing a mandate);
  - The personal data is necessary to honour a legal obligation of Van Lanschot Kempen (e.g. client assessment with a view to accepting a new client, providing information to the Tax Authority, providing information to government and regulatory bodies);
  - The personal data is needed in respect of a legitimate interest of Van Lanschot Kempen, unless the interests of the concerned party's privacy prevail (e.g. marketing activities, combating fraud, risk management);

- The processing of personal data is also permitted when the party concerned has given their unambiguous consent for one or more specific purposes (e.g. by ticking a box next to a statement to the effect that the personal data can be used for certain clearly defined purposes).

- *Personal data cannot be retained any longer than necessary*
  Van Lanschot Kempen has described the retention periods and guidelines on clearance in its Retention and Clearance Policy ("Beleid bewaren en schonen" version 1 May 2018).

- *Personal data must be protected against loss or any form of illegitimate processing by providing for appropriate technical and organisational measures*
  The Information Security Policy ("Informatiebeveiligingsbeleid") of Van Lanschot Kempen describes the principles for securing information, including personal data, at Van Lanschot Kempen.

- *Information duty vis-à-vis parties concerned and rights of parties concerned*
  Before processing personal data, Van Lanschot Kempen has to inform the parties concerned as to the purpose for which it is collecting data of the party concerned and, if this data has not been obtained directly from the party concerned itself, how Van Lanschot Kempen has obtained the data.
  Van Lanschot Kempen should inform the client at the moment when the latter enters into a contract with Van Lanschot Kempen (with a reference to the privacy statement). This Privacy Statement includes an explanation of the rights of the parties concerned and how they can exercise these rights.

  Prospects should be informed at the very first moment of contact.

  Van Lanschot Kempen should inform members of staff when it offers them an employment contract. To that end, staff members will be given a copy of the local Regulation on Processing Personal Data.

  Applicants should be informed when they apply for a vacancy through the website.

  Visitors of the websites of Van Lanschot Kempen should be informed that the websites make use of functional, analytic or tracking cookings. The website visitors have to choose which cookie settings they prefer. Information about the cookies settings can be consulted.

The above, as well as other principles, are also described in the document entitled "Privacy by Design", which can be retrieved from Wiki/Compliance/Privacy.

Requirement

The business is obliged to conduct a Privacy Impact Assessment (hereinafter: PIA) prior to engaging in any novel type of personal data processing. A novel type of personal data processing could arise, for example (but not exclusively), when developing or purchasing an automated system, introducing a new service or product, developing smart data solutions (possibly but not necessarily in combination with profiling), deploying new technologies, outsourcing an existing process, or contracting a service from an external provider.

A PIA is a method for assessing the privacy risks to which parties concerned may be exposed when their personal data is processed, and for establishing what measures should be taken in order to mitigate these risks. Van Lanschot Kempen should not process personal data if the PIA reveals a High Residual Risk. There is a High Residual Risk when Van Lanschot Kempen is unable to reduce the concerned parties' privacy risk to an acceptable level by taking appropriate protective measures.
The PIA also provides Van Lanschot Kempen with an important method for demonstrating that personal data is processed according to the legislation and regulation in force.

To support this process, Van Lanschot Kempen has introduced a Privacy Impact Assessment procedure. This procedure comes with a checklist that the business can use to assess the risks to the privacy of our clients, prospects, persons linked to clients and contacts for business relations posed by the processing of personal data for the purpose of providing a new type of service or adjusting an existing service. The Privacy Impact Assessment procedure can be retrieved from Wiki/Compliance/Privacy.

The Privacy Impact Assessment procedure covers the Privacy by Design and Privacy by Default principles.

3. Specific principles

3.1 Recording personal data of prospects

Specific rules apply for collecting, recording and storing personal details of prospects. These rules are specified in the document entitled “werkinstructie inzake vastleggen toestemming ihkv Algemene Verordening Gegevensbescherming”. This document can be accessed at Wiki/Compliance/Privacy.

Requirement

The business should draft procedures guaranteeing compliance with the rules stated in the document “werkinstructie inzake vastleggen toestemming ihkv Algemene Verordening Gegevensbescherming”. This mainly concerns rules in relation to the duty of information, the initial recording, approval, and clearance of this personal data.

3.2 Recording personal data of applicants

Specific rules apply for the collecting, recording and retaining of personal data of applicants. One important reason is that the data of an applicant who has been rejected for the vacancy in question should be deleted from the systems of Van Lanschot Kempen within 4 weeks following completion of the application process. The rejected applicant can give permission for this personal data to be retained for a further period of at most 12 months, in case a matching vacancy arises during that period.

Requirement

3.3 The business should draft procedures that guarantee compliance with the aforementioned rules. Recording of personal data of clients, persons linked to clients and contacts of business relations

In accordance with the general principles, Van Lanschot Kempen can process the personal data of these groups of individuals in its systems, because of the underlying contractual relationship. When collecting and recording data, Van Lanschot Kempen staff must not lose sight of the original purpose of collecting personal data. The recording of personal data in the CRM systems of Van Lanschot Kempen deserves specific attention in this regard (contact moment). This recording must be relevant for service provision and in principle should not include special personal data, unless the party concerned has given explicit consent for the processing of this data. Special personal data is among other things data on health, political preference, race, religious beliefs, sexual

orientation and data on union membership. With some exceptions, the GDPR does not permit the recording of such special personal data.
Van Lanschot Kempen has determined that, in principle, no special personal data may be recorded in the bank's CRM systems, unless the party concerned has given explicit consent for the processing of this data. If doing so would serve a purpose or would be necessary in the context of maintaining or managing the relationship (for example to send a little something to the client in case of either illness or dementia in an investment service relationship), the staff member should be careful in registering the specific detail. The staff member should not record more information than is strictly necessary and should use neutral and general phrases as much as possible in such records.

Requirement

There are no further requirements for the business, other than ensuring that there is sufficient awareness about this section. As stated explicitly in Section 4, it is management's responsibility to ensure sufficient awareness among the staff.

3.4 Rights of parties concerned

The party concerned is the party to whom personal data relates. The party concerned has a number of rights. These are as follows:

- Right of access
  A party concerned has the right to ask the bank whether it is processing his/her data and request a copy of such a record.
- Right to rectification
  A party concerned has the right to have his/her personal data corrected and expanded in the event that incorrect or incomplete personal data has been processed.
- Right to object
  A party concerned can object to the processing of his/her personal data for reasons relating to his/her personal situation.
- Right to restriction of processing
  The party concerned has the right to request that the bank temporarily suspend the processing of his/her personal data.
- Right to erasure ('right to be forgotten')
  In some cases, the party concerned has the right to request that Van Lanschot Kempen delete his/her personal data.

- Right to data portability
  The party concerned can request the personal data from the bank for personal use or can ask the bank to transfer this personal data to a third party.

The Privacy Statement, which can be accessed on the website of the various units of Van Lanschot Kempen, explains how the party concerned can make a request in view of one of these rights.

Requirements

- Such a request from the party concerned can be received by an individual member of staff.
- If the request is made by telephone, the staff member must refer the party concerned to the website, which explains how the request can be submitted.
- If the request is submitted in writing, the staff member should forward it by e-mail to privacyofficer@vanlanschotkempen.com.
- Following receipt of the request, the Privacy Officer will consult Legal Affairs to determine whether and how the request can be met.
- The Privacy Officer informs the manager of the organisational unit, as well as the staff member who forwarded the request, of the processing of the request and final handling of the request.
- The manager of the organisational unit informs the party concerned of the final outcome of the request.

3.5 Data leaks

Van Lanschot Kempen is under obligation to notify the regulatory body (the Dutch Data Protection Authority) of any breaches of security resulting in, for example, the theft, loss or abuse of personal data (referred to as a data leak). This concerns data leaks which constitute a risk to the right of protection of the personal sphere (privacy) of the party concerned:

Examples of data leaks:

- Hacking of the Van Lanschot Kempen system whereby personal data is stolen;
- Loss of a laptop, memory stick, tablet, etc. containing personal data. The same applies to the loss of paper files containing personal data;
- Mailing large volumes of personal data to the wrong e-mail address;
- etc.

Requirement

Every member of staff at Van Lanschot Kempen who detects a data leak must immediately report this to the postbox Meldpunt Datalekken Postbus. (postbox data leakage notification) or click on the incident button on the intranet homepage. The documents "Q&A, what to do in the event of a data leak" and "Background information on data leaks notification duty" provides a succinct description of what a data leak is and what staff should do when they detect a data leak. The "Procedure Meldplicht Datalekken" (data leak notification duty procedure – available in Dutch only) provides further details. All documents can be found at Wiki/Compliance/Privacy.

3.6 Marketing

It is in Van Lanschot Kempen's commercial interest to establish and maintain direct contacts with its clients and attract new clients (direct marketing). The use of personal data of clients and prospects for the purpose of direct marketing is permitted if certain conditions are met.
The conditions under which the personal data of prospects can be used for the purpose of direct marketing as well as the rules that must be followed when approaching prospects are laid down in the document entitled "werkinstructie inzake vastleggen toestemming ihkv Algemene Verordening Gegevensbescherming". This document is available at Wiki/Compliance/Privacy.

When clients are contacted for marketing purposes, they should always be informed about the possibility of unsubscribing from any further advertising. Whenever Van Lanschot Kempen intends to approach clients for marketing purposes, it should verify whether the client unsubscribed for this purpose at an earlier stage.

Requirements

- The business should provide a system and procedures for registering the right of prospects and clients to object to being contacted for marketing purposes, and ensure that this register is consulted before contacting prospects and clients.
- The business should provide procedures to ensure that the right of objection is included in (e-)mailings, and that clients and prospects are explicitly reminded of this right when they are contacted by telephone.

3.7 Outsourcing activities – engaging processors

Van Lanschot Kempen can outsource activities to third parties (one example being the printing and distribution of bank statements). This outsourcing can involve the processing of personal data. If the third party processes personal data on instruction from Van Lanschot Kempen, this third party is referred to in legislation as the processor. This third party has no independent say over the personal data which Van Lanschot Kempen has provided for the purpose of carrying out the activities concerned.

Van Lanschot Kempen has to enter into a processor's agreement with this third party. The processor's agreement contains all the important topics that are relevant for the protection of personal data and which the third party needs to comply with.

The processor's agreement includes agreements about the following:

- The purpose of the processing
- The prohibition of using the personal data for other purposes
- The security of the personal data
- The retention period and deletion of the personal data
- The notification duty in the event of security incidents and data leaks
- The right to conduct an audit at the third party to verify whether the terms of the agreement are upheld.

The processor's agreement can be accessed at Wiki/Compliance/Privacy.

If the third party is not based in the EU, additional rules are in force concerning the processing of personal data. The rules for processing personal data are stricter when the third party is based in a jurisdiction outside the EU. (This also applies for locations where the data is stored and if the data can be accessed from a jurisdiction outside the EU).

Requirements

If the business decides to outsource to a third party any activities that involve personal data, the business must:

- Conduct a risk analysis and a Privacy Impact Assessment in order to determine whether the processor offers sufficient guarantees in respect of the security of personal data, and whether the processor will honour the obligations that follow from the agreement.
- Make unambiguous agreements about the purpose of the processing, and only provide the data needed for that specific purpose (data minimisation).
- Ensure that a processor's contract is drafted by Procurement, possibly in consultation with Legal Affairs.

4. Tasks and responsibilities of Van Lanschot Kempen staff

Management

Management has the following responsibilities:

- Translate the principles stated in this requirements document into processes, procedures and operating instructions, as needed;
- Inform the staff about the requirements document and ensure that they are sufficiently aware of its content, possibly enlisting the support of the Privacy Officer to that end
- Be a role model in dealing with personal data
- Ensure compliance with the principles stated in this requirements document.

Staff

Van Lanschot Kempen staff are responsible for complying with the principles stated in this document. In practice, this responsibility amounts to the following:

- The staff should understand and be aware of the content of this requirements document and the procedures and operating instructions derived from it. Questions can be addressed to management or to the Privacy Officer;
- The staff should correctly apply the principles stated in this requirements document and the procedures and operating instructions derived from it;
- When in doubt as to the proper application of this requirements document in any given situation, the question concerned should be addressed to management or to the Privacy Officer;
- Non-compliance with the principles stated in this requirements document must be reported to management and to the Privacy Officer.

Privacy Officer

The Privacy Officer has the following responsibilities:

- Make this “Privacy, protection of personal data” requirements document available to staff;
- Advise on the application of the requirements document in day-to-day operations and translate it into processes, procedures and operating instructions;
- Regularly review the requirements document and update it as needed;
- Monitor the proper implementation of and compliance with the principles stated in the requirements document;

- Support awareness-building in the business.

5. Evaluate the requirements document

5.1 Related documents

The following documents are related to this requirements document.

- "Het beleid bewaren en vernietigen" (Retention and clearance policy)
- "Het informatiebeveiligingsbeleid" (Information security policy)
- "Procedure Meldplicht Datalekken" (Policy relating to the data leaks notification duty)

This documents are only available in Dutch.

Other privacy-related documents can be found at Wiki/Compliance/Privacy.

5.2 Regular review

Compliance will review the "Privacy and protection of personal data" requirements document once every three years and in the event of major changes.