Global Data Privacy Policy

Wolters Kluwer

Document control

Name of Policy	Global Data Privacy Policy
Short description	This overarching Policy sets the framework for how Wolters Kluwer companies comply with data protection legislation, including the data privacy principles to adhere to when handling personal data within Wolters Kluwer.
Policy Owner	Global Law and Compliance Department
Contact details	privacyoffice@wolterskluwer.com
To whom this Policy is binding	All Wolters Kluwer companies
Approval level	Executive Board
Effective date	March 1, 2024

Version history

Version control				
Version number	**Last review (year)**	**Last Amendments**	**Changes at last amendments**	**Approved by**
1.0	2024	n/a	n/a newly established	Executive Board
2.0		January 2025	Non-material editorial refinement and supplemental examples incorporated.	

Content

1 Scope and purpose of this Policy

Wolters Kluwer is committed to safeguarding the personal data of our customers, workforce members and other stakeholders in compliance with applicable data privacy legislation and in line with its Code of Business Ethics. This Global Data Privacy Policy (this "Policy") provides the data privacy principles that should be adhered to when handling personal data within Wolters Kluwer.

The data privacy principles set out in this Policy are generally accepted standards for processing personal data, as derived from the European Union's General Data Protection Regulation ("GDPR"). The GDPR is Wolters Kluwer's global data privacy baseline and is internationally recognized as providing a high level of protection to personal data.

This Policy applies to all Wolters Kluwer companies. "Wolters Kluwer" or a "Wolters Kluwer company" refers to Wolters Kluwer N.V. and its subsidiaries and group companies in which Wolters Kluwer holds a majority interest or the right to appoint management. Wolters Kluwer companies are responsible for implementing local policies, procedures, standards or guidelines as applicable for its workforce members to ensure compliance with data privacy legislation and in line with this Policy. In certain circumstances, a Wolters Kluwer company may be required to enact a policy regarding data privacy with stricter requirements or requirements set by applicable data privacy legislation that differ from those contained herein. Workforce members that work for such Wolters Kluwer companies will receive notice of the additional requirements and will receive training based on their role.

This Policy has been approved and adopted by the Executive Board of Wolters Kluwer N.V.

2 Privacy governance

As part of Wolters Kluwer's data privacy program, Wolters Kluwer has implemented a hybrid data privacy governance model with certain functions centralised whilst having teams supporting day-to-day operations within the businesses.

Wolters Kluwer has a centralised privacy function within the Global Law and Compliance Department, along with dedicated privacy roles within the businesses, including Data Privacy Managers, Privacy Champions and Data Protection Officers (where applicable).

The Corporate Privacy team within the Global Law and Compliance Department leads the global data privacy compliance program for Wolters Kluwer, including overseeing the strategic direction and day-to-day operations of the privacy program, acting as the primary point of contact for data protection authorities, and providing guidance on new and amended privacy laws and regulations. Where required, the Corporate Privacy team will develop and maintain Wolters Kluwer's data privacy policies and procedures and advise Wolters Kluwer on adherence to sound and effective data management practices.

The Data Privacy Managers support the data privacy program to ensure organizational compliance with applicable data privacy legislation by overseeing the data management practices in their businesses. The Data Privacy Managers are supported by Privacy Champions who are responsible for the implementation and maintenance of the data privacy policies and procedures in their businesses in line with the requirements set out in this Policy.

Where required by applicable data privacy legislation, or as otherwise decided by Wolters Kluwer to voluntarily do so, Wolters Kluwer has appointed Data Protection Officers or Privacy Officers for certain

businesses. In accordance with their assigned responsibilities as defined by applicable data privacy legislation, they will work together with the Privacy Champions and Data Privacy Managers of their respective businesses.

Within Wolters Kluwer, usual audit cycles are implemented to ensure evaluation of data privacy compliance. Audits are conducted periodically by both Data Privacy Managers (as part of local risk management and managerial oversight) as well as Internal Audit as an operations independent function.

3 Personal data processing

Wolters Kluwer will adhere to the data privacy principles described in this Policy when processing personal data. The concepts of personal data and processing derive from data privacy legislation and are described in more detail below.

3.1 Personal Data

Personal data refers to all person-identifiable information, including direct identifiable information such as name, address or phone number. The concept of personal data also includes information that can be linked in any way (including via the combination with additional information) to an individual, such as location data, descriptions of behaviour, or unique identifiers such as an IP address or personnel number.

Sensitive data is a subcategory of personal data that reveals details that could be used to discriminate against or cause harm to the individuals identified, such as information concerning someone's race, health, political opinions or sex life, sensitive financial information such as credit card data, or national identification numbers. Sensitive data requires extra care and a stricter level of handling than personal data, depending on the requirements following applicable data privacy legislation.

Example

When onboarding an employee, a company requests a copy of the person's passport, carrying out the obligation to verify the identity of the new employee. Such photo IDs typically contain sensitive data and can only be processed if a specific statutory exemption applies.

Personal data at Wolters Kluwer can include personal data of workforce members (present, past and prospective), [contact persons at] customers, end users, contractors, suppliers and other business partners with whom a Wolters Kluwer company has a relationship.

3.2 Processing

Processing is broadly defined and encompasses any action in relation to personal data during its life cycle. For example, collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, accessing or otherwise making available, alignment or combination, restriction, erasure or destruction.

This Policy applies to any processing of personal data undertaken by any Wolters Kluwer company by electronic means and in systematically accessible paper-based filing systems.

3.3 Roles of Data Protection

For each processing of personal data by a Wolters Kluwer company, the roles and responsibilities of each of the actors in the processing chain should be determined. The qualification of each actor will determine the responsibilities of each party under applicable data privacy legislation.

The qualification of the actors in the processing chain requires an assessment of the factual circumstances of the processing of personal data. The party that decides how and why personal data is processed will, in most cases, primarily be required to comply with the obligations set out under applicable data privacy legislation. Under GDPR this party qualifies as a data controller, however, the qualification and naming convention can differ in other jurisdictions. The deciding party may delegate the processing of personal data to a third party that processes personal data on behalf of the deciding party. Under the GDPR, this party qualifies as data processor, although this designation and naming convention can also vary by jurisdiction (i.e. in California, this would be referred to as a "service provider").

For example, with respect to the processing of personal data from workforce members and direct business relations (such as contacts at suppliers or customers), Wolters Kluwer will be the deciding party and therefore needs to directly comply with the obligations following from the applicable data privacy legislation.

With respect to the processing of personal data from end users of its customers, Wolters Kluwer processes the personal data on behalf of its customers and therefore in many circumstances qualifies as a data processor, but the qualification can differ in other jurisdictions or be dependent on how the product is offered.

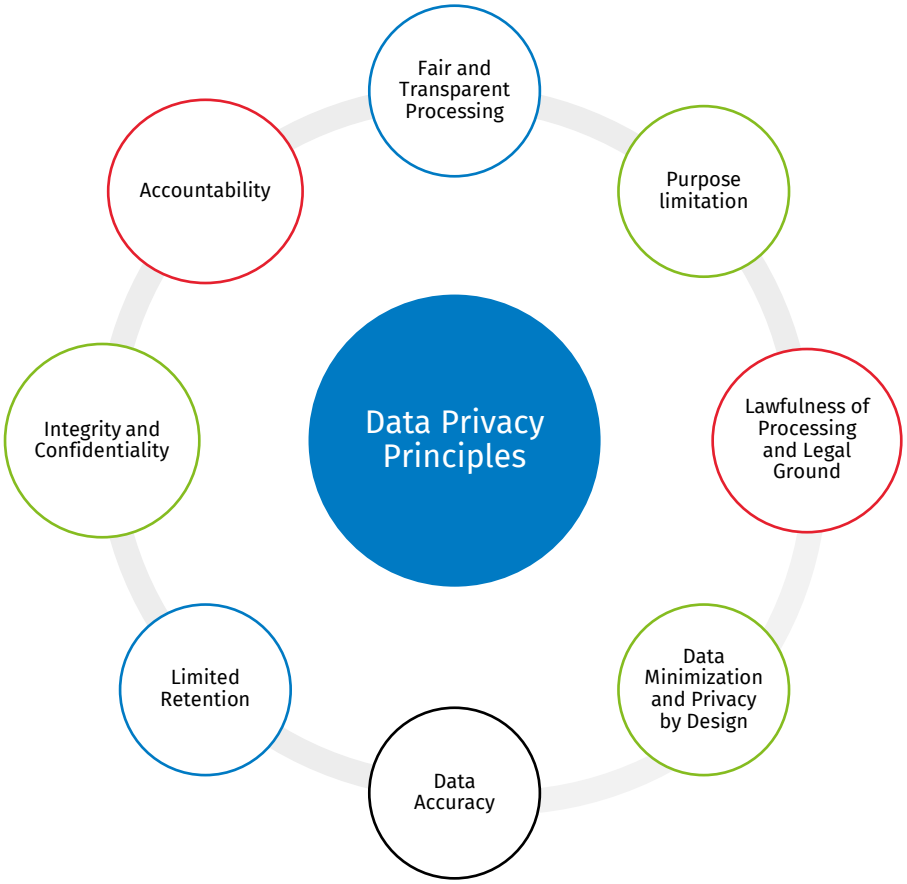
Examples

A company takes the role of data controller when using a vendor management tool to process personal data on its vendors based in the EU, which enables it to control vendor expenditure.

A company selling Software-as-a Service (SaaS) to customers based in the EU who can then upload certain personal data of their customers into the SaaS system is a data processor for the purposes of providing these software services.

4 Data privacy principles

Data privacy principles are generally accepted standards for processing personal data. These principles are often embedded in data privacy legislation. Wolters Kluwer will observe these data privacy principles when processing personal data. This Policy gives a general description of each of the data privacy principles and helps to ensure that all personal data is processed fairly, transparently, safely and securely. These data privacy principles are described in more detail below.



4.1 Fair and Transparent Processing

Personal data must be processed fairly and in a transparent manner. In light of this principle, the reasonable expectations of the individuals concerned and the effect that the processing may have on them should be taken in consideration. The transparency requirement means being open about the processing, so that the individuals are aware of what personal data is collected and processed, for what purposes, and who is responsible for the processing. Another important aspect of transparency is informing the individuals about their rights and how they can exercise those rights. Section 6 of this Policy provides more information about these rights.

Wolters Kluwer has different privacy policies to ensure that its workforce members, website visitors and job applicants are duly informed on the processing of their personal data by Wolters Kluwer.

Example

A company sells products online in its web shop. When customers visit the web shop and purchase a product, the company collects and, thus, processes their personal data. Before the customers purchase a product, the company presents them with a privacy policy, explaining how it uses their personal data when visiting the web shop and in the context of the execution of the purchase.

4.2 Purpose limitation

The principle of purpose limitation means that personal data can only be collected for specified processing purposes. The purposes for which personal data are collected should be specified no later than at the time of the personal data collection. The subsequent processing of this personal data is limited to the fulfilment of those collection purposes or such other purposes that are compatible with the collection purposes. If the new purpose is not compatible with the collection purposes, a new processing ground (see section 4.3) is to be selected and applied. The purpose(s) of processing should be documented in a record of processing as further described in Section 5 below.

4.3 Lawfulness of Processing and Legal Ground

Each processing of personal data requires a valid processing ground to be lawful, depending on the applicable data privacy legislation. The processing ground is the legal basis on which the processing of the personal data takes place.

For example, the following are the lawful processing grounds for processing under the GDPR (some of which may also be recognized under other jurisdictions' data privacy legislation):

Ground 1 - Performance of a contract

Processing that is necessary to perform contractual obligations or pre-contractual measures, including commercial contracts with customers, suppliers, and business partners.

Examples

Before the signing of a contract: To conclude a customer service contract, a company asks the customer to provide their name and contact details of the customer's representatives which are ***necessary*** for the company to draft and finalize the customer service contract.

During the term of a contract: A customer requests a service provider to add an additional user to have access to the platform. Therefore, the name and email of the user will be shared with the service provider and the service provider will add the user in accordance with the agreed process.

Ground 2 - Compliance with a legal obligation

Processing of personal data that is necessary to comply with a legal obligation to which a company is subject.

Example

Copies of invoices are retained for the specified time period in accordance with tax and bookkeeping requirements. A company generates and archives the invoices (which include personal data about the customer) to comply with its legal obligations.

Ground 3: - Protecting vital interests of an individual

Protecting the 'vital interests' of an individual is a very limited processing ground. It generally only applies to processing necessary personal data to ensure an individual's safety and wellbeing during emergency situations when they are unable to give consent.

Example

A visitor who accesses the premises of a company suddenly faints on arrival at the reception. The receptionist checks the individual's pockets, finds in the visitor's pocket a Diabetes card and follows the instructions.

Ground 4: - Legitimate interests

Processing that is for the company's legitimate interests provided that appropriate assessments have occurred to balance the legitimate interest against the privacy rights and freedoms of the individual. This may include consideration as to whether the individual would reasonably expect that processing of their personal data may take place in the specific business context.

Example

A company that has considered the privacy of its customers by way of an appropriate assessment, may analyze certain customer feedback and interactions, to the extent necessary and proportionate, to improve its products and services. This processing helps the company understand customer needs and enhance their experience.

Ground 5 - Consent from the individual

Processing of personal data by the company where the individual has provided consent for the specific processing of their personal data. Under GDPR and privacy laws in many other jurisdictions, consent must be freely given, informed, specific, an affirmative act, and unambiguous, with the option to withdraw such consent at any time.

Example

An individual fills out a form on a company's website with some of their personal data to receive more information about the products offered by the company. As part of the online form, the individual provides their consent by ticking a box on the form that states that the individual may be contacted by the company for this purpose. The individual's information is then processed by the company for the purpose of marketing communications based on the consent provided.

4.4 Data Minimization and Privacy by Design

The principle of data minimization means that personal data processed must be adequate, relevant, and limited to the personal data that are necessary for the purposes of the processing activity. Wolters Kluwer will only process personal data if necessary and share personal data if there is an actual need-to-know.

Wolters Kluwer will ensure, when developing new systems and processes, that privacy aspects are considered during the design phase.

Example

An online product of a company is used by 50 individual customers. The system does log IP addresses and credentials but does not keep record of the names of the individuals that used the product and how long each page was open. This information proved not to be necessary for system management and data security purposes.

4.5 Data Accuracy

This principle of data accuracy means that personal data is accurate and kept up to date on a regular basis. When Wolters Kluwer becomes aware of any inaccuracies, it will correct or delete the personal data without undue delay. Individuals who become aware of inaccuracies in their personal data must be given the opportunity to report this and, where necessary based on proof of any inaccuracy, have it corrected. Wolters Kluwer will periodically review and update the personal data that it processes to ensure that the personal data it holds is accurate, up to date and relevant.

Examples

An employee recently married and has taken the last name of the spouse. The employee informs the HR department of their company of the changed last name and submits any legally required supporting documentation. HR will update this information in the system. In locations where a self-service portal is implemented, employees can also check the correctness of their data themselves and update as needed, after submitting any supporting evidence, where necessary.

A customer informs a company that the customer's account manager has moved to another work location and the telephone number is changed. The updated telephone number is recorded in the company's customer database.

4.6 Limited Retention

The principle of limited retention means that personal data will not be kept for longer than necessary or as required by law. Retention periods set forth the length of time certain personal data may be kept. The length of the retention period depends, in part, on the type of personal data and the purposes for which it has been obtained. When determining the retention period for certain personal data, legal record-keeping requirements must be considered. Countries, state and local laws may provide specific minimum or maximum data retention periods, thus requiring certain personal data to be retained for a shorter or longer

period of time. If Wolters Kluwer is processing personal data on behalf of its customers, the retention period applicable to the personal data is as agreed with the customer.

The personal data stored must be reviewed regularly and Wolters Kluwer will delete or de-identify the personal data, if the personal data is no longer required or if the agreed upon retention period ends. As an alternative to deletion, data may be kept by Wolters Kluwer in a format in which it is no longer possible to identify the individual; for example, by anonymization of the personal data.

Example

A company retains a visitor log for visitors to the premises. The personal data recorded in the visitor log will be deleted in accordance with specified retention periods taking into account any retention requirements prescribed by law (which may vary from country to country (and state to state)).

4.7 Integrity and Confidentiality

The principle of integrity and confidentiality requires that personal data must be processed in a safe and secure way. This includes for, example, the protection against unauthorized access to the personal data or damage to the personal data. Wolters Kluwer is responsible for implementing appropriate technical and organizational measures to keep personal data secure. These measures vary and depend on the type and sensitivity of personal data that is processed. The measures should be determined on a case-by-case basis and determined based on the categorization of the personal data.

Examples

An example of a technical security measure is to enable encryption on desktops, laptops, or mobile phones.

An example of an organizational measure is that workforce members in certain roles may be required to sign a separate confidentiality agreement because of the sensitivity of the tasks assigned to them.

4.8 Accountability

When acting as data controller, Wolters Kluwer is responsible for demonstrating ('accountability') compliance with the applicable data protection legislation of which the data privacy principles described above can form an important part.

When acting as data processor, the instructions set out in the contractual agreement with the customer will primarily determine the responsibilities for Wolters Kluwer.

Irrespective of when Wolters Kluwer acts as data controller or data processor, Wolters Kluwer recognizes that correct and lawful treatment of personal data contributes to the success of the business and maintains the trust of its stakeholders.

Wolters Kluwer has set up a privacy control framework, consisting of a set of privacy controls, aimed to mitigate relevant privacy risks possibly involved with the processing of personal data. The objective of the privacy control framework is to set a robust privacy baseline for all Wolters Kluwer's jurisdictions based on the data privacy principles.

5 Assessments

Assessments are a way of complying with the accountability principle referenced in paragraph 4.8 above. The data processing activities are recorded and the level of risk for the individual in relation to the processing of personal data are assessed.

5.1 Data Mapping

A record of processing activities assessment (RoPA) is a data-mapping exercise whereby Wolters Kluwer creates a comprehensive record of its processing activities that contain personal data. It serves as an internal control tool and provides a way for Wolters Kluwer to demonstrate compliance with applicable data privacy legislation, depending on the country or state.

5.2 Data Protection Impact Assessment and Triage

A data protection impact assessment (DPIA) is an instrument that can be used to analyze, identify and minimize privacy and data protection risks of a processing activity that involves personal data within Wolters Kluwer. A data protection impact assessment can also help to identify measures that mitigate those risks. Depending on the applicable data privacy legislation, performing a data protection impact assessment is a key element of complying with the accountability principle in paragraph 4.8 above.

A triage is a short assessment to establish whether there is a need for Wolters Kluwer to perform a data protection impact assessment for a particular processing activity.

6 Individual rights

Depending on the local applicable data privacy legislation, an individual whose personal data is collected and processed by Wolters Kluwer, has certain rights in relation to their personal data.

Examples of such rights are:

(a) **The right to access – the right to have a complete overview of personal data of the individual.**

> **Example:**
>
> A website visitor who has downloaded a product whitepaper, is requesting access to their personal data left on the website of the company owning the website. The company checks what details are (still) on record and provides these details following the request in accordance with the applicable privacy notice and applicable local laws.

(b) **The right to rectification – the right to change incorrect personal data.**

> **Example:**
>
> A customer finds out that their contact details are incomplete or incorrectly recorded in the customer database of a company. The customer requests the company to update the database with the correct contact details.

(c) **The right to erasure – the right to have personal data removed.**

> **Example:**
>
> A customer who signed up for a conference a year ago and agreed to receive information about similar organized events by a company, is no longer interested. The customer requests to delete all personal data the company has on record.

(d) **The right to object – the right to object to certain activities such as direct marketing or consent-based processing.**

> **Example:**
>
> A company uses personal data to send direct marketing emails and mail flyers to encourage individuals to purchase the company's products and services. Recipients of these emails and flyers may object to receiving these marketing communications.

7 Incident management

A data privacy incident is a security incident that occurs when data protection (security) controls have or may have been circumvented, did not work or were not available, resulting in the loss of or exposure to unauthorized persons of personal data. As part of Wolters Kluwer's Global Incident Management Program, Wolters Kluwer has a specific data privacy incident management plan, which enables multi-disciplinary incident management teams around the globe to agilely respond to, manage, and communicate about the data privacy incident. The qualification of a data privacy incident may differ based on applicable data privacy legislation.

If a data privacy incident occurs where Wolters Kluwer is directly processing the personal data (and thus acts as data controller), Wolters Kluwer may have a legal requirement to notify a supervisory authority based on applicable data privacy legislation. In certain cases, Wolters Kluwer is also obliged to communicate the data privacy incident to the individuals involved.

If a data privacy incident occurs where Wolters Kluwer is indirectly processing personal data on behalf of customers (and thus acting as data processor), Wolters Kluwer will inform the relevant data controller in a timely manner in accordance with the obligations in applicable data privacy legislation and the contractual obligations in place with customers.

8 Sharing of personal data

8.1 Sharing Personal Data internally

In the context of daily business operations, personal data is processed, such as personal data from employees, business contacts, customers, or suppliers and may be shared between entities within Wolters Kluwer. The data protection role of the sharing Wolters Kluwer company and the receiving Wolters Kluwer company, either a data controller or data processor, depends on the specific situation of personal data sharing and determines the level of data protection obligations imposed on such entities.

8.2 Sharing Personal Data with third parties

Wolters Kluwer shares personal data on a regular basis with third parties which it has contracted with for services, for example with third parties of IT solutions used within Wolters Kluwer. Wolters Kluwer has set up a supply chain risk management process for engaging with a third party, which includes the completion of a due diligence process when selecting the third party, the assessment of the third party for compliance with Wolters Kluwer's minimum requirements and a review of necessary contractual documentation.

Before sharing any personal data with a third party, Wolters Kluwer will conclude appropriate contractual arrangements with such third party. Depending on the data protection roles of Wolters Kluwer and the third party and the requirements under the applicable jurisdiction(s), this can be by means of a data processing agreement or legal equivalent.

9 International transfers

As Wolters Kluwer may share personal data with other Wolters Kluwer companies or with third parties located globally, the transfer of personal data from one country to another can be restricted or subject to additional conditions. For example, Wolters Kluwer has executed an Intra-Group Data Transfer Agreement and standard contractual clauses for the transfer of personal data legally between other Wolters Kluwer companies. Similarly, the provisions required to be included in agreements between Wolters Kluwer and third parties receiving personal data may vary based on the jurisdictions involved.

Example:

A company with subsidiaries in the EEA uses a third-party vendor management system to administer its workflow and purchase orders. The supplier of this system is a company located in the United States and the system runs on the supplier's servers, located in the US. When the company uses the system and enters records, personal data is transferred to the supplier located outside the EEA. Additional measures must be put in place, for example through the use of a data protection agreement containing the standard contractual clauses adopted by the European Commission and other technical and organizational measures to protect the personal data transferred.

10 Enforcement and compliance

Wolters Kluwer provides training to all relevant workforce members on data privacy matters including the data privacy principles upon initial induction and on a regular basis thereafter. This training is mandatory, and completion of the training will be monitored by Wolters Kluwer.

Violations of applicable data privacy legislation can result in significant financial fines and reputational damages for Wolters Kluwer and its customers.

Any workforce member having knowledge of any conduct inconsistent with this Policy or violation of this Policy shall promptly report such matter to their manager or higher manager, the Corporate Privacy team within the Global Law and Compliance Department, or the Ethics & Compliance Committee via the SpeakUp line or email ecc@wolterskluwer.com. Wolters Kluwer has a zero tolerance for retaliation. This means that reporters are protected for raising a concern in good faith. See the Code of Business Ethics for more information.

11 Policy Updates

This Policy will undergo annual review unless regulatory or business needs dictate otherwise. The GLCD is responsible for reviewing and updating this Policy. Any substantive changes to this Policy will be reviewed by the Executive Board.

Annex 1

Definitions list

Data controller	A natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
Data privacy incident	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.
Data privacy legislation	All laws and regulations applicable to the processing of personal data throughout the world as assessed by Wolters Kluwer in a particular processing situation, which can include without limitation: • GDPR; • ePrivacy Directive: the provisions of Directive 2002/58/EC of 12 July 2002 ("Directive on privacy and electronic communications") or, as applicable, any successive legislation that repeals and replaces this directive; • National implementation laws: any and all applicable national implementation laws of the aforementioned European laws; • In relation to the UK, the UK General Data Protection Regulation (as incorporated into the UK law since January 2021) and the Privacy and Electronic Communications (EC Directive) Regulations 2003; • Other privacy laws and regulations: any and all applicable national, federal, state or local laws and regulations anywhere in the world related to data protection and privacy matters.
Data processor	A natural or legal person, public authority, agency, or other body which processes personal data on behalf of the data controller.
Workforce or workforce member(s)	Everyone who works for a Wolters Kluwer company including board members, officers, employees and contractors.
End users	Users of products of Wolters Kluwer, which have been purchased by customers of Wolters Kluwer.
GDPR	Regulation (EU) 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).

Individuals	The natural person (individual) whose personal data is processed.
Personal data	All person-identifiable information, including direct identifiable information and indirectly identifiable information.
Processing	Any action in relation to personal data during its life cycle, including collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, access or otherwise making available, alignment or combination, restriction, erasure or destruction.
Sensitive data	A subcategory of personal data that reveals details that could be used to discriminate against or cause harm to the individuals identified, such as information concerning someone's race, political opinions or sex life, sensitive financial information such as credit card data, or national identification numbers.