

PRIVACY AND GDPR COMPLIANCE

Background

The GDPR applies to the processing of personal data. Personal data is defined as any information relating to an identified or identifiable natural person and includes data such as an IP address, an email address or a telephone number. Processing activities include, among others, the collection, use and disclosure of the data.

The GDPR provides for additional protection to the processing of special categories of personal data. Such special categories include, personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership and genetic and biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

According to the GDPR, personal data must be processed in accordance with the principles of lawfulness, fairness and transparency. In addition, such data must be collected for specified, explicit and legitimate purposes and not further processed in an incompatible manner to those purposes (principle of purpose limitation).

A data controller or a data processor must also make sure to respect the principle of data minimization, meaning that personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they were processed. Personal data must be accurate and, where necessary, kept up to date. In addition, the accountability principle is recognized itself as a fundamental principle.

Finally, the principles of storage limitation and integrity and confidentiality have to be respected. Therefore, personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed and must be processed in a manner that ensures appropriate security of the personal data.

What We're Doing

We're not collecting more data or using your personal data any differently. All we're doing is complying with the GDPR because we take data privacy, processing, sharing and storage extremely seriously at Straker.

We're completely transparent on how we use the information we collect, how long we keep that data, and the rights you have regarding it.

GDPR gives businesses around the world a chance to update how they manage their communications to customers, how they comply with the new laws and how they can improve customer services. By using Straker Translations Limited (**Straker**) and Straker subsidiaries (**the Straker Group**) services, you're agreeing to the data privacy and security laws of the GDPR.

Lawfulness of processing

Under the GDPR, a processing of personal data will only be lawful if, at least one of the conditions below is met:

- the data subject has provided consent to the processing,
- 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,
- the processing is necessary for compliance with a legal obligation to which the controller is subject,
- the processing is necessary to protect the vital interests of the data subject or of another natural person, or
- the processing is necessary for the performance of a task carried out in the public interest
- the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

This is what we've been doing to be GDPR compliant

- Accessing all our data sources through traditional data warehouses, structured and unstructured data, data at rest and data in motion to establish what personal data is being stored by us.
- Inspecting all data resources to establish what personal data can be found. This includes extracting, categorizing and cataloguing personal data elements such as first names and last names, email addresses and company names.
- Documenting and sharing new GDPR/privacy rules across all areas of the business. Strict governance ensures personal data can only be accessed by those with proper rights, based on the nature of the personal data, the rights associated with user groups and the usage context.
- Establishing the correct levels and techniques to protect data: through either encryption, pseudonymization and anonymization based on the user's rights and the usage context.
- Producing reports for independent auditors to verify what personal data we have, where it's located, that we properly manage the process for getting consent from individuals who are involved; proof of how personal data is used, who uses it and for what purpose; and that all appropriate processes are in place to manage data breaches and security issues.

Our accountability

When you interact with Straker and/or the Straker Group, we may collect personal data from you - such as when you request a quote, email us with a translation enquiry, subscribe to our newsletters or contact our customer service representatives or use certain Straker and the Straker Group services.

When you interact with us through our services, we receive and store certain information such as an IP address, device ID, and your activities within the services. We may store such information, or such information may be included in databases owned and maintained by us.

The services may use such information and pool it with other information to track, for example, the total number of visitors to our websites.

Please refer to our Privacy Policy on our website.

We do not sell your information to third parties under any circumstances.

Your Rights

As a data subject, you have the following rights under the GDPR:

- The right to information requires data controllers to give individuals certain information about the processing of their personal data free of charge (exceptions apply - Article 14). This information must be provided in a concise, transparent, intelligible and easily accessible form using clear and plain language. Data controllers can provide such information to individuals in combination with standardized icons to give an easily visible, meaningful overview of the processing.
- The right to be forgotten, also referred to as the right to erasure as it includes both the right to have the data erased and the right to delisting in certain circumstances. The individuals have the right to require data controllers to delete their data in certain circumstances, including where the information is no longer necessary for the purpose for which it was collected or where the individual withdraws their consent and there is no other legal grounds for processing their data.
- The right to restriction of processing applies in some specific circumstances including for example, for an interim period allowing the data controller to verify the accuracy of the personal data that is contested by the data subject, or when the controller no longer needs the personal data for the purposes of the processing but are required by the data subject for, for example, the establishment of legal claims.
- The right to data portability refers to the right of an individual to receive personal data that he/she has provided to the data controller in a structured, commonly used and machine readable format and to transmit that data to another data controller without hindrance. This right only applies to personal data that an individual has provided to the controller, where the processing is based on the individual's consent or for the performance of a contract and where the processing is carried out by automated means. The exercise of this new right to data portability shall be without prejudice to the exercise of the right to erasure or the right of access.

If you have any comments, concerns or complaints about our use of your personal data, please contact us on dataprivacy@strakergroup.com.

We will respond to any rights that you exercise as soon as possible in receipt of your request, unless the request is particularly complex or cumbersome, in which case we will respond within six months (we will inform you within the first month if it will take longer than one month for us to respond).

Data Submission, Storage, User Uploads and Services

If you no longer consent to our processing of your personal information (in respect of any matter referred to in our Privacy Policy as requiring your consent), you may request that we cease such processing by contacting us on dataprivacy@strakergroup.com.

Please note that if you withdraw your consent to such processing, for example in respect of the use of cookies, it may not be possible for us to provide all / part of the Service to you.

In the case of data uploaded by a data controller (and not the data subject), and Straker and/or the Straker Group is the data processor, any withdrawals of consent must be made by the relevant data subject to the data controller, and the data controller can then instruct Straker and/or the Straker Group to take action in relation to the processing of the data subject. This can mean that it may not be possible to continue to use Straker and the Straker Group services in respect of said data.

Straker and the Straker Group will not share your personal information without your consent or unless required by law (except as set out in this Privacy and GDPR Compliance policy).

Withdrawal of Consent

By the nature of our service, Straker and the Straker Group may gather statistical information and store that information. This may include information that does not identify you individually.

If Straker and the Straker Group becomes involved in a merger, acquisition, or any form of sale of some of all of its assets, we will provide notice before personal information is transferred to any third-party. This may include information that does not identify you individually.

As Straker and the Straker Group is a data processor, we will only process such data subject's personal data in accordance with our instructions from the relevant data controller in accordance with the Terms of Service or Services Agreement in place between Straker and/or the Straker Group and the data controller.

We may share with third-parties certain pieces of aggregated, non-personal information such as the number of sites, devices accessed while using Straker and/or the Straker Group, for example. This may include information that does not identify you individually.

We restrict access to personal information to employees, vendors and associates who need to know that information in order to operate, develop, or improve our services. These individuals are bound by confidentiality obligations and may be subject to

discipline, including termination civil litigation and/or criminal prosecution, if they fail to meet these obligations.

Your personal information may be transferred to, stored at, or accessed from a destination outside the European Economic Area (**EEA**) for the purposes of us providing the Service. It may also be processed by staff operating outside the EEA who work for us, another corporate entity within our group, or any of our suppliers.

By submitting your personal information, you explicitly consent to this transfer, storing or processing. We will take all steps reasonably necessary to ensure that your personal information is treated securely and in accordance with this Policy.

The safeguards in place with regard to the transfer of your personal information outside of the EEA are the entry by us into appropriate contracts with all transferees of such data.

All information you provide to us is stored in our (or contracted third-party) secure servers. Where we have given you (or where you have chosen) a password which enables you to access the Service, you are responsible for keeping this password confidential. We ask you not to share a password with any person not authorized to use the Service.

The sources and organizations to which we share information are also GDPR compliant. The information we share may include first name, last name and email address. If you want to delete this information we can contact the source on your behalf.

Storage and Destruction of Previous Translations

We may store the documents related to your translation job (source documents, supporting documents, translated documents) in our system for a maximum of 2 years from the time the job is created. After this period, all documents related to your job will be securely and permanently destroyed from our system.

Legal Information

Straker respects the privacy of our visitors and customers. We have therefore established a Privacy Policy to assist you to understand what information we collect and how that information is used.

What personal information does Straker collect?

The type of information we will collect about you, but not exclusively, includes:

- Your name
- Address
- Phone number
- Email address
- Credit/debit card details if you are paying in this manner
- Credit information – if you are engaging with our services as a business and wish to set up a credit account

- Credit/debit card details will be collected but, unlike other details, will not be held on our database. Your credit card information will be stored with our third-party online secure payment processing provider Windcave (www.windcave.com).

If you are quoted for a job that requires a deposit and balance to be billed at the end, then your card will be charged for the remaining figure (quote minus deposit already paid) on completion of the job and prior to the translated files being released. You will be notified by email that the completion payment has been processed. For more details on this secure storage see <https://sec.windcave.com/pxmi3/privacy-policy>

On Straker's websites you can request information about our services, download marketing or support materials, chat online with an expert, and request pricing quotes. The types of personal information you provide to us on our websites may include names, employer, addresses, phone numbers, and e-mail addresses.

Secure Industry-Recognized Controls

Straker is committed to taking reasonable efforts to secure the personal information you choose to provide to us. To protect the privacy of any personal information you may have provided, Straker employ industry- standard controls including physical access controls and internet firewalls.

We are certified to ISO17100 certification standards – which replaced the EN15038 standard in October 2015 and is the highest global quality standard for translation services. To comply with this certification, our document relay systems, internal processes and professional translators are stringently tested and evaluated.

Archiving and Previous Translations

Our system automatically archives all source, Supporting and Translated Files 2 years after the job status is set to 'Completed'. All Source, Supporting and Translated Files are then securely destroyed following this 2-year period.

Website Cookies and Third-Party Websites Cookies

A cookie may contain information (such as a unique user ID) that is used to track the pages of the websites you've visited. This information is stored in a safe and secure database. You can refuse cookies by turning them off in your browser.

Straker does use "cookies" on its websites. Cookies are identifiers that can be sent from a website via your browser to be placed on your computer's hard drive. Thereafter when you visit a website, a message is sent back to the web server by the browser accessing the website. You may elect not to accept cookies by changing the designated settings on your web browser. However, not utilising cookies may prevent you from using certain functions and features of websites.

The information collected from the use of cookies is used and analysed to improve Straker's websites. Straker uses the information collected from the "cookies" to collect the pages visited, navigation patterns, etc. of a visitor. This information helps us answer

questions such as “What information is of most interest to our customers?” and “What kind of services do our customers require?”

The Straker websites may provide links to third-party websites for your convenience and information. If you access those links, you will leave the Straker website. Straker does not control those sites or their privacy practices, which may differ from Straker’s. We do not endorse or make any representations about third- party websites. The personal data you choose to give to unrelated third-parties is not covered by the Straker Privacy Policy.

Please refer to Straker Cookie Policy for full details.

Contact Information

For more information on our current Privacy Policy and GDPR compliance, you may wish to contact us directly: dataprivacy@strakergroup.com

If you have any questions or believe that the privacy of your personal information has not been respected, you may submit a complaint in writing to the attention of the Data Privacy Officer Manager at Straker’s corporate headquarters in PO Box 305110, Triton Plaza, Albany, North Shore City 0757, New Zealand.