WiseTech GLOBAL

Data Privacy Policy

An Information Services Document

WiseTech GLOBAL

Introduction

WiseTech Global Limited and its subsidiaries (**WTG, we, our, us**) recognize the importance of data privacy. This data privacy policy (the **policy**) shall apply to all employees who handle or have access to personal data, in particular personnel in the People and Culture, Information Services, Business Development, and Marketing and Partner Management departments who collect and process personal data. This may include sensitive and highly confidential data such as details of employment relationships, salary, disciplinary procedures, health information including illness or disability, performance-related information, and any other relevant personal data. WTG considers it crucial to apply the highest standards of data privacy at all times.

Local legislation in your jurisdiction might impose even more strict standards regarding the protection of personal data than those outlined in this policy. Local legislation prevails over this policy if and to the extent that it exceeds the standards of this policy, imposes stricter requirements, and/or provides more protection for data subjects.

This policy documents WTG's data privacy principles. Its purpose is to create understanding and awareness of data privacy issues that you might face because of your employment with us.

Personal data shall be…

processed based on **legal grounds**	processed in line with **data subjects' rights**	processed in a **transparent manner**
Processed for **limited** and **legitimate purposes** only	**Adequate**, **relevant,** and **necessary**	**Accurate** and **up to date**
Secure and **confidential**	**Kept no longer than necessary** for the legitimate purposes	**Transferred to third parties only if permitted by law** and subject to appropriate agreements

I. Background

1. The EU General Data Protection Regulation

To harmonize European and national data protection regulations across Europe, the EU General Data Protection Regulation (**GDPR**) will come into force with effect as of 25 May 2018. The GDPR will be directly applicable and enforceable in all Member States of the European Union and has cross-border reach for entities that control or process data of subjects who are in the EU, which includes WTG.

2. Penalties

The GDPR applies penalties in the event of a breach of GDPR provisions. Penalties may be up to **EUR 20,000,000** or up to **4 percent of annual worldwide turnover**, whichever is higher, in the event of an infringement.

3. Scope of application

The GDPR applies to:

- the processing of personal data by a data controller or a data processor located in the EU, **regardless of whether the processing takes place in the EU or not**; and
- the processing of personal data of data subjects who are in the EU by a controller or processor not established in the EU, where the processing activities are related to
  - the offering of goods or services to such data subjects in the EU; or
  - the monitoring of their behavior as far as their behavior takes place within the EU.

II. Key terms explained

1. Personal data

Any information relating to an identified or identifiable natural person (**personal data**), which means information from which a person can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier, and so on. Examples include name, residential address, photograph, telephone number, email address, and social security number.

2. Special categories of personal data

There are also special categories of personal data. These include data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as data concerning health or sexual orientation. This kind of information may also be referred to as “sensitive data.”

3. Data processing

Any operation or set of operations that is performed on personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, and erasure or destruction.

4. Data subject

Any living individual (that is, a natural person) to whom the personal data or special categories of personal data relates, which may include current and former employees, job candidates, other workers including contractors, employees' next of kin and beneficiaries, and business contacts at customer organizations or suppliers.

5. (Data) Controller

The natural or legal person who, alone or jointly with others, determines the purposes and means of the processing of personal data. For instance, as your employer we process your personal data as a controller.

6. (Data) Processor

The natural or legal person who processes personal data on behalf of a controller. In some cases a service provider that is engaged by the company might act as a processor on behalf of the company. In other cases, the company might act as a processor on behalf of one of its customers. If you consider this to be the case in a specific situation related to your work, please inform the company's Data Privacy Coordinator and the Data Privacy Officer, where applicable.

III. Prohibition to process personal data

It is important to understand that the processing of personal data is prohibited unless there is a legal justification.

Justifications include:

- The need to fulfil a contract with the data subject. For example, employers may process applicants' or employees' data insofar as this is necessary for hiring decisions or for carrying out or terminating the employment contract.
- The pursuit of the company's or a third party's legitimate interests. In this case, data processing can still be prohibited if the data subject has an overriding legitimate interest in their data being excluded from processing.
- A legal obligation that the company is discharging. For example, employers can be required to make disclosures to social security institutions.
- The data subject's voluntary and informed consent.
- Court orders and instructions of authorities may also constitute a possible justification. If you receive such an order or instruction please inform the Data Privacy Coordinator or the Data Privacy Officer, where applicable.

Before collecting and/or processing personal data it must be assessed if there is a legal justification. It is therefore encouraged to contact the Data Privacy Coordinator or the Data Privacy Officer, as appropriate, in good time.

IV. Transfer of personal data outside of the EU/EEa

The legality of a transfer of personal data outside of the EU/EEA[1] must meet two tests:

[1] The European Economic Area (**EEA**) includes EU countries as well as Iceland, Liechtenstein, and Norway.

- Personal data may be transferred to a third party only if there is a legal justification (outlined in clause III) for such a transfer to occur;
- Additionally, a data transfer outside of the EU/EEA is permissible to recipients where there is an adequate level of data protection.
    - The European Commission compiled a “white list” of countries where an adequate level of data protection is guaranteed.
    - A data transfer to countries not on this list (in particular, to the United States) requires additional safeguards, such as:
        - Standard Contractual Clauses issued by the EU Commission which are to be incorporated into the data processing agreement with the recipient;
        - Binding Corporate Rules; or
        - the EU-U.S. Privacy Shield.

Before transferring personal data outside of the EU/EEA it must be assessed if there is a legal justification and if the recipient guarantees an adequate level of data protection. It is therefore encouraged to contact the Data Privacy Coordinator or the Data Privacy Officer, where applicable, in good time.

V. Common data privacy issues

1. Monitoring of employees

When employees are to be monitored it must first be assessed:

- if the monitoring of employees is permissible; and
- if any legal requirements are to be satisfied before monitoring occurs

Monitoring of employees may include screening, reviewing and monitoring of emails (including spam filters), monitoring internet use (including the ability to deny access to certain websites), monitoring of phone usage to charge costs to employees, monitoring of mobile devices including their localization via GPS and video surveillance etc.

In some jurisdictions the works council (which does not exist in Australia) will be involved before employees may be legally monitored.

2. Using third party providers

It must be ensured that all service providers are held to high data privacy standards when processing Personal Data of WTG’s employees or customers.

Third party providers must be selected carefully. Before entering into an agreement with a third party provider please contact the Data Privacy Coordinator or Data Protection Officer to ensure the contractual framework provides for appropriate data protection.

3. Transferring personal data to other group companies

Before transferring data to another entity within the WTG Group contact the Data Privacy Coordinator or the Data Privacy Officer, where applicable, to ensure the appropriate legal framework is in place. Please note: granting remote access to IT systems is considered a data transfer and so the same rules apply.

Personal data of employees may require involvement of the works council or other employee representatives before an agreement is concluded and the data is transferred.

4. Implementing new IT systems / new software

Before implementing new IT systems or new software that processes personal data you must contact the Data Privacy Coordinator and/or the Data Privacy Officer as soon as practicable to make sure requisite procedures are followed. Please also refer to clause VIII below. In certain jurisdictions this may also require the involvement of the works council before the IT system or new software is rolled out or used.

VI. How to handle personal data

1. Avoiding personal data breaches

Enforce physical security of documentation:

- Limit and control access to work areas by visitors.
- Lock away documentation, keep offices and work stations in orderly condition so that it is easy to identify whether something is amiss.
- Retrieve sensitive documents from printers as soon as possible, or where possible, use secure printing facilities.
- Lock cabinets and drawers that contain sensitive materials, for example, personnel files.

Enforce IT security:

- Ensure that access to databases and systems is controlled and well maintained including measures such as regular data backup.
- Use password protection on all devices, including mobile devices.
- Do not share your passwords with others.
- Encrypt emails that contain sensitive personal information.
- Do not use unsecured or vulnerable computers, removable storage devices or public / unprotected WiFi networks.

2. Data subjects' rights

Under the GDPR, WTG must provide information to data subjects about its processing of personal data, unless the data subject already has this information. The information must be provided in a concise, transparent, intelligible, and easily accessible form, using clear and plain language. Information must be

provided at the time WTG obtains information directly from the data subject, and within a reasonable period of having obtained the data when the data is not obtained directly from the data subject.

The data subjects also have a right to obtain information about data processed about them, access to such data, and rectification of inaccuracies in their personal data.

Data subjects may ask to receive their personal data in a structured and commonly used, machine readable format so that the data can be easily transferred to another data controller.

When collecting personal data directly or indirectly, ensure that notice is given at the appropriate time to the data subject.

3. Right to erasure/ right to be forgotten

Under the GDPR, data subjects have the right to ask for the erasure of their personal data if certain conditions apply. WTG has the obligation to erase personal data without undue delay in circumstances which may include:

- the personal data is no longer necessary in relation to the purpose/s for which it was collected or otherwise processed;
- the data subject withdraws the consent on which the processing is based and where there is no other legal reason for the processing and no overriding legitimate reasons for the processing;
- the personal data has been unlawfully processed;
- the personal data must be erased to comply with a legal obligation of the controller.

Where WTG has made the personal data **public**, it must take reasonable steps, including technical measures, to inform other parties processing the personal data of the data subject, that the data subject has requested the erasure of any links to, or copy or replication of, that personal data.

Before making any personal data public, such as on WTG's website, the right to be forgotten, and the time, effort, and costs of a potential obligation to erase such personal data should be considered carefully. Before making any personal data public, you may contact the Data Privacy Coordinator to ensure that this is done correctly.

4. Period of personal data storage

Personal data stored should be adequate, relevant, and limited to what is necessary for the purposes for which they are processed. This requires ensuring that the period for which the personal data is stored is limited to a strict minimum (in accordance with the applicable local laws and corresponding retention periods). Time limits should be established for erasure or for a periodic review, ensuring that personal data is kept no longer than necessary in accordance with the relevant applicable local laws and retention periods, if any exist.

When destroying documents in accordance with the above, documents containing personal data should be shredded or disposed of securely through a suitably licensed document destruction service provider.

VII. Data mapping

To prepare for and comply with the extensive record keeping duties under the GDPR, an inventory of all data processing activities must be established and it must be verified whether the requirements for each processing activity under the GDPR are met. All relevant WTG departments, the Data Privacy Coordinator and the Data Privacy Officer (where applicable), should participate to ensure completeness and compliance with the GDPR.

To prepare the inventory the following steps must be taken:

- All processes where personal data is collected and processed, including by third party service providers, must be listed.
- A distinction based on the relevant countries must be made, i.e. (1) processes within one country, (2) cross-border processes within the EU/EEA and (3) processes in or concerning third countries.
- The legal basis for every processing activity must be determined and documented.
- It must be verified if a Data Protection Impact Assessment (**DPIA**) is required. That is the case where a type of processing, in particular, using new technologies and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the rights and freedoms of data subjects in case of processing special categories of personal data on a large scale – for more details please see VIII.

VIII. Data Protection Impact Assessment (DPIA)

1. When to conduct a DPIA

When using IT systems, software or hardware such as cameras or GPS systems for the processing of personal data, WTG must evaluate carefully if a DPIA must be conducted.

A DPIA should always be considered when the data processing meets any of the following criteria:

- Personal data concerning employees is processed.
- The data processing concerns the data subject's performance at work.
- A systematic monitoring of data subjects occurs, e.g. by installing cameras or by monitoring the internet use.
- Special categories of data are being processed.
- Personal data is being processed on a large scale.
- Personal data is being transferred to third countries outside the EU / EEA.

  Please note that local data protection authorities will publish a list of data processing activities that will definitely require a DPIA. This list must be adhered to.

2. How to conduct a DPIA

The DPIA must be carried out prior to the processing of personal data. It should be started as early as practical and must be monitored and, if necessary, updated at a later stage if there are changes to the data processing. In some cases the DPIA will be an on-going process, e.g. when the data processing is dynamic and subject to ongoing change.

WTG is responsible for ensuring that the DPIA is conducted and must seek the advice of the Data Protection Officer, where designated. If the data processing is wholly or partly performed by a data processor, the processor should be asked to assist the company in carrying out the DPIA and provide any necessary information.

The DPIA must be documented in writing and contain at least the following:

- a description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
- an assessment of the necessity and proportionality of the data processing;
- an assessment of the risks to the rights and freedoms of data subjects;
- the measures envisaged to address the risks and demonstrate compliance with the GDPR.

Please note that WTG might have to seek the views of data subjects or their representatives (e.g. the works council). The GDPR does not define a process for seeking those views, they can therefore be sought through a variety of means, depending on the context.

Please inform the Data Privacy Coordinator and/or the Data Privacy Officer as soon as practicable if you think that a DPIA may be required in order for them to conduct or coordinate the assessment and align with the relevant supervisory authority, if required.

IX. Drafting and maintaining records of processing activities

To comply with the extensive record keeping requirements under the GDPR, records of the processing activities must be kept and maintained. The records need to be available to the supervisory authority upon request.

- Records must be kept in writing, including electronic form.
- A process must be implemented to ensure that records are kept up to date, e.g. responsible individuals from relevant departments must be appointed, deadlines for regular reviews must be defined etc.
- The GDPR provides for the necessary content of such records. In the case of a controller, the necessary content is:
    - the name and contact details of the company, the joint controller (if applicable), the controller's representative and the Data Protection Officer (if applicable);
    - the purposes of the processing;
    - a description of the categories of data subjects and of the categories of personal data;

- the categories of recipients to whom the personal data has been or will be disclosed, including recipients in third countries or international organizations;
- where applicable, transfers of personal data to a third country or an international organization, including the identification of that third country or international organization and, if applicable, the documentation of suitable safeguards;
- where possible, the envisaged time limits for erasure of the different categories of personal data;
- where possible, a general description of the technical and organizational security measures.

X. Privacy by design / privacy by default

Data privacy shall be embedded into any processing of personal data that is deployed. Under the GDPR, WTG must adopt internal policies and implement technical and organizational measures that provide by default:

- only personal data which is necessary for each specific purpose of the processing is to be processed. That obligation applies to the amount of personal data collected, the extent of its processing, the period of its storage and its accessibility, and
- that personal data is not made accessible to more individuals than necessary for the purpose.

Please note that this requirement applies to the implementation of new IT systems, but also to any IT systems that are already in use at the company and accordingly, the settings of all IT systems must be reviewed and, if necessary, amended in accordance with the above guidelines.

XI. Local contact person / Data Privacy Coordinator

A local contact person has been appointed for each business site. This local contact person is familiar with the details of data privacy requirements at the relevant site and will act as a point of contact for data subjects and data privacy authorities. The local contact person will merely act as a point of contact but the site manager remains responsible for data privacy compliance at the site.

You can contact the Data Privacy Coordinator and their team using the following email address privacyofficer@wisetechglobal.com.

XII. Handling personal data breaches

A personal data breach means 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. The company will typically be required to notify such a data breach to the competent supervisory authority without undue delay, and where feasible, not more than 72 hours after having become aware of it. In some cases, the company must also notify the affected data subjects without undue delay.

Personal data breaches must be reported immediately to the Data Privacy Coordinator at the following email address privacyofficer@wisetechglobal.com

Do not try to resolve a personal data breach yourself.