Privacy notices for the usage of FUTURA Engineering

Requirements of the European General Data Protection Regulation (GDPR)

1. Introduction

Futura Solutions GmbH (hereinafter referred to as 'Futura Solutions') develops and operates the cloud-based purchasing and procurement platform FUTURA®, which is used to digitally interconnect business processes between purchasers (hereinafter referred to as “customer”) and external actors, i.e., service providers, partners, and suppliers (hereinafter referred to as “users”). This technical communication basis, provided by means of a browser, enables the exchange of information and documents (hereinafter referred to as 'information') for the purpose of collaboration.

In the cloud-based purchasing and procurement platform FUTURA®, personal data is necessarily collected and stored by the business partner (“customer”) of “user” for specific purposes defined by “customer”. In this respect, “customer” is primarily the “controller” in the sense of the EU General Data Protection Regulation (GDPR) (see Art. 4 para. 7) by collecting the personal data of “user”. “Futura Solutions” in turn processes data on behalf of the “customer” and is therefore a “processor” in the sense of the GDPR (see Art. 4 para. 8). For this reason, a contract has been concluded with “customer” for commissioned data processing in accordance with Art. 28 GDPR.

In the course of the activation of the user account (hereinafter referred to as 'account') by ‘user’, the latter has the possibility to change the personal data collected by ‘customer’. In this respect, with the activation of the 'account' by the ‘user’, the 'user' becomes responsible for the personal data originally collected by the ‘customer’.

The protection of natural persons with regard to the processing of personal data is a fundamental right. The GDPR considers this as well.

“Futura Solutions” fully implements the regulations of the GDPR as “processor” towards “customer” and “user”. “Futura Solutions” maintains a list of processing activities in accordance with Art. 30 GDPR (see Appendix 03).

“Futura Solutions” ensures that data and in particular personal data is stored within the European Union (EU) and that there is no transfer of this data to third countries.

As a “processor”, “Futura Solutions” also guarantees that personal data is protected and that the rights of the data subjects are observed if they fall within the area of responsibility of a “processor”.

2. Definition of terms (GDPR) – Art. 4 (excerpt)

For the purposes of the Regulation, the terms “personal data” or “data subject”, “controller” and “processor” are defined as follows:

(1) “personal data” means any information relating to an identified or identifiable natural person (“data subject”); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

(2) “controller” means the 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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

(3) “processor” means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

(4) “consent” of the data subject means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

3. Acknowledgement and confirmation process

These privacy notices must be acknowledged by “user” in the course of the activation of their user account (hereinafter referred to as “account”). In addition, "user" must confirm the General Terms of Use. The acknowledgement as well as the confirmation must be made prior to the initial registration or prior to a registration after a possible change of the privacy notices or the General Terms of Use.

The acknowledgement and confirmation are logged. Without this acknowledgement and confirmation, registration and ultimately the usage of the FUTURA® cloud service is not possible.

Upon activation of the “account” by “user”, the user himself becomes the “controller” of the personal data originally collected by “customer”.

4. Rights of data subjects

4.1 Information concerning the protection of personal data

The following passage contains information about the protection of personal data of the data subject as laid down in Articles 13 and 14 (GDPR):

Quote from GDPR	**Information**
n/a	If you have any questions or concerns regarding the protection of personal data, please contact the Futura Solutions support first. You can reach it as follows: Futura Solutions GmbH Kreuzberger Ring 68 65205 Wiesbaden Germany Phone: +49 611-33460-460 E-mail: support@futura-solutions.de
Art. 13: 1 (a) the name and the contact details of the controller and, where applicable, of the controller's representative;	The name and the contact details of the "controller" of your business partner can be found in the respective e-mail invitation or system notification concerning the corresponding business transaction or activity.
Art. 13:1 (b) the contact details of the data protection supervisor, where applicable;	The contact details of the respective data protection supervisor of the "controller" can be found in the respective e-mail invitation or system notification concerning the corresponding business transaction or activity.
Art. 13: 1 (c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;	The purpose and legal basis for the processing of personal data consists in the digitization of business processes and procedures of "controller", intended to interconnect the "data subject" with the business transactions or activities of "controller". The legal basis for this is Art. 6 para. 1 lit. b) DSGVO.
Art. 13: 1 (d) where the processing is based on point (f) of Article 6 (1), the legitimate interests pursued by the controller or by a third party;	The legitimate interests of "controller" for storing personal data result from the need to record business processes for auditing purposes. The data is stored only for the statutory retention periods.
Art. 13: 1 (e) the recipients or categories of recipients of the personal data, if any;	The following parties are recipients or categories of recipients of personal data or have access to it: · Employees of the controller (the controller specified in the e-mail invitation or system message mentioned above) · Administrators of the above-mentioned controller · Employees of Futura Solutions GmbH, Wiesbaden
Art. 13: 1 (f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organization and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49 (1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.	"Controller" will not transmit personal data to a third country or international organization.
Art. 13: 2 (a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;	The personal data is stored for the duration of the statutory retention periods. Otherwise, the data will be deleted as soon as storage is no longer required.
Art. 13: 2 (b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;	"User" has the right to obtain information about the personal data in question from the "controller" and to request rectification, erasure, limitation of processing or to object to processing, as well as the right to data transferability. The personal data entered into FUTURA® by the "user" can also be modified and deleted by them.
Art. 13: 2 (c) where the processing is based on point (a) of Article 6 (1) or point (a) of Article 9 (2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;	"User" has the right to withdraw the consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal. For this purpose, "user" must contact the "controller".

Art. 13: 2 (d) the right to lodge a complaint with a supervisory authority;	“User” has the right to file a complaint with the respective supervisory authority. The contact details of the supervisory authority in charge of the “controller” can be found in the respective e-mail invitation or system notification. However, a complaint can be filed with any data protection supervisory authority.
Art. 13: 2 (e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data; Continued in the following section	The provision of personal data on FUTURA® is not a statutory or contractual requirement. “User” is not obliged to provide personal data. Consequences of not providing personal data are that “user” cannot participate in “controller's” business transactions or activities on this platform.
Art. 13: 2 (f) the existence of automated decision-making, including profiling, referred to in Article 22 (1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.	No automated decision-making is carried out on this platform.
Art. 14: 1 (d) the categories of personal data concerned;	Categories of personal data that is processed are the following: · First name, last name, username (for logging on to the application) · Connection data (log data, IP address) · Description e.g., function in the company · Department · E-mail address · Phone · Fax · System Language
Art. 14: 2 (f) from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;	In the case that “user” has not submitted personal data in FUTURA® themselves; "controller" must disclose to "user" the source from which the personal data has been collected.
Art. 14: 3 (b) if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject;	The personal data is to be used for communication with “user”, in particular for the invitation to participate in business transactions or activities.
Art. 14:3 (c) if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.	“Controller” informs “user” if they intend to disclose personal data to another recipient.

4.2 Automatic erasure of personal data

4.2.1 Erasure of personal data of “users” who have never participated in a business transaction or activity

In the event that an account with personal data has been created for a “user” (“data subject”) for the purchasing and procurement platform FUTURA®, if the “user” does not take note of the privacy notices provided there and at the same time does not agree to the Terms of Use provided in the same place and/or also objects to the processing of personal data, or if the “user” does not respond to the "controller's" invitation to complete the registration process and activate the account within a certain period of time, this account with the personal data collected by the “controller” will be automatically deleted. The deadline for this is 90 days after the “controller” has sent the invitation

About the procedure: The initiator or “controller” of a business transaction or business activity creates a new “user” (“data subject”) in the purchasing and procurement platform FUTURA® and collects personal data for this purpose. FUTURA® then automatically generates an account and sends the access data to the registered e-mail address. The access data is sent via e-mail

“User” now has 90 days to react or register. They will be reminded of this within the 90 days and will be informed about the consequence, namely that the created “account” will be automatically deleted after this period.

4.2.2 Erasure of personal data of “users” who have participated in a business transaction or activity at least once

“Account”, including all personal data of “user” who has participated at least once in a business transaction or activity will be deleted automatically after expiration of the statutory retention period following their last participation in a business transaction or activity.

The statutory storage obligations are regulated in contracts between “customer” and “Futura Solutions”.

The rights, in particular the right to information of “data subjects” in accordance with the GDPR are unaffected by this.

Appendix 01 – Technical and organizational measures (TOM)

1. Confidentiality (Art. 32 para. 1 lit. b GDPR)

- **Equipment access control**
  No unauthorized entrance to data processing facilities, e.g.: magnetic or chip cards, keys, electric door openers, plant security or gatekeepers, alarm systems, video systems;
- **Login control**
  No unauthorized system usage, e.g.: (secure) passwords, automatic locking mechanisms, two-factor authentication, encryption of media;
- **Data access control**
  No unauthorized reading, copying, modification or removal within the system, e.g.: Authorization concepts and customized access rights, logging of hits;
- **Separability**
  Separate processing of data collected for different purposes, for example: multi-client capability, sandboxing;
- **Pseudonymization (Art. 32 para. 1 lit. a GDPR; Art. 25 para. 1 GDPR)**

The processing of personal data in such a way that the data can no longer be assigned to a specific data subject without the inclusion of additional information, provided that this additional information is kept separately and is subject to appropriate technical and organizational measures, e.g.: the replacement of the name and other identifying features with a mark for the purpose of excluding or significantly complicating the identification of the data subject.

1. Integrity (Art. 32 para. 1 lit. b GDPR)

- **Disclosure control**
  No unauthorized reading, copying, modification or removal during electronic transmission or transport, e.g.: encryption, Virtual Private Networks (VPN), electronic signature;
- **Input control**
  Determining if and by whom personal data in data processing systems has been entered, modified or removed e.g.: Logging, document management;

1. Availability and resilience (Art. 32 para. 1 lit. b GDPR)

- **Availability control**
  Protection against accidental or willful destruction or loss, e.g.: Backup strategy (online/offline; on-site/off-site), uninterruptible power supply (UPS), virus protection, firewall, reporting channels and emergency plans;
- **Resilience**

Data processing systems must be so resilient that their functionality is guaranteed even under intensive traffic and heavy workloads e.g.: reducing the error-proneness of individual system components, increasing agility through virtualized system components and resources;

- **Fast restorability (Art. 32 para. 1 lit. c GDPR)**

The ability to restore the availability of and access to personal data quickly in the event of a physical or technical incident. For example, implementing a contingency management with the description of the strategic approach, via e.g., a contingency management guideline and/or policy, the as-is analysis of business impacts and risks and a corresponding implementation plan as well as a contingency prevention concept, business continuity planning, a restart plan and the execution of multi-stage contingency tests.

1. Procedures for regular review, assessment and evaluation (Art. 32 para.1 lit. d GDPR; Art. 25 para. 1 GDPR)

- **Data protection management system (DSMS)**

Procedures for regular review, assessment and evaluation, e.g.: implementation of a data protection management system (DSMS) with the description of the strategic approach, for example, by means of a data protection management guideline and/or policy, creation of lists of processing activities (in accordance with Art. 30 para. 2 GDPR), preparation of privacy notices, elaboration of erasure concepts as well as regular auditing of the planned and taken measures by an external data protection officer.

- **Incident-response-management**

Firewalls, spam filters as well as virus scanners are used, which are updated regularly. Furthermore, IDS and IPS systems are used.

- **Privacy-friendly presets (Art. 25 para. 2 GDRP)**

Measures are in place to ensure privacy-friendly presetting. The exercise of the right of withdrawal can be carried out by technical means.

- **Processing control**
  No commissioned processing within the meaning of Art. 28 GDPR without corresponding instructions from the client, e.g.: clear contract design, formalized order management, strict selection of the service provider, obligation to convince in advance, follow-up checks.

Appendix 02 – List of processing activities in accordance with Art. 30 EU-GDPR

I. General

'Futura Solutions', in the role of a "processor", has drawn up a list of processing activities in accordance with Article 30 paragraph 1 of the GDPR, with the following content:

1. The name and contact details of the "processor" and the data protection officer.
2. The purposes of the processing.
3. A description of the categories of data subjects and the categories of personal data
4. The categories of recipients to whom the personal data have been or will be disclosed, including recipients in third countries or international organizations.
5. Where appropriate, transfers of personal data to a third country or international organization, including an indication of the third country or international organization concerned, and, in the case of transfers referred to in the second subparagraph of Article 49 para. 1, the documentation of appropriate safeguards
6. If possible, the deadlines specified for the erasure of the various categories of data.
7. If possible, a general description of the technical and organizational measures referred to in Article 32 para. 1.

The information in section 1 shall precede the contents of the individual processing operations.

II. List of processing activities

a. Contact details

Below you will find the contact details of 'Futura Solutions' as "order processor" as well as the contact details of the external data protection officer of 'Futura Solutions:

Details of the processor (Art. 30 para. 2 lit. a)
Futura Solutions GmbH Kreuzberger Ring 68 65205 Wiesbaden Germany
Phone.: +49 611 33460-300 E-mail: dataprotection@futura-solutions.de Internet: http://www.futura-solutions.de

Details of the data protection officer

DEUDAT GmbH Herr Mario Arndt Zehnthofstraße 5b 65205 Wiesbaden Germany
Tel.: +49 611 950008-32 E-Mail: mario.arndt@deudat.de Internet: http://www.deudat.de

b. Description of processing

The purpose and category of processing operations carried out on behalf of a customer are listed below:

Description of data processing				**Providing of the cloud-based purchasing and procurement platform FUTURA® via the internet**							
Purpose	**Category**	**Legal basis**	**Data subjects**	**Personal data**	**Recipients and authorized parties**	**Privacy Impact Assessment (PIA)**	**Risk management, analysis of protection requirements**	**Data processing equipment**	**Third Country Transfer**	**Standard periods for erasure**	**General description of TOM**
Performing a business transaction	Cloud-Service	Art. 6, para. 1, lit. b EU-GDPR	Employees of the customer's suppliers and his service providers	According to contract for data processing according to Art. 28 EU-GDPR agreed upon with the customer	Employees of the customers and employees of Futura Solutions	Is carried out according to Art. 35 EU-GDPR	Confidentiality, availability, integrity: each very high	Server, Laptop, Computer	No!	All data, including personal data, will be treated and deleted in accordance with the contractual agreement with the customer.	See Annex 1, Contract for order processing according to Art. 28 EU-GDPR