d.velop

Privacy Policy
for products and services from d.velop AG

Contents

1. General information ... 3
   1.1 Controller ... 3
2. Definitions ... 3
   2.1 Definitions from the GDPR ... 3
   2.2 Definitions for cookies and similar technologies ... 3
   2.3 Definitions for data categories ... 4
3. Information about data processing ... 4
4. Legal basis for the processing of personal data ... 4
5. Duration of storage ... 4
6. Contact channels (support) ... 4
7. Social media login (signing up for a user account using a Facebook account) ... 5
8. Proper use of our products and services, billing ... 5
9. Ticket system ... 6
10. Rights of the data subject ... 6
   10.1 Right of access according to Art. 15 GDPR ... 6
   10.2 Right to rectification according to Art. 16 GDPR ... 7
   10.3 Right to erasure according to Art. 17 GDPR ... 7
   10.4 Right to restriction of processing according to Art. 18 GDPR ... 7
   10.5 Right of notification according to Art. 19 GDPR ... 8
   10.6 Right of data portability according to Art. 20 GDPR ... 8
   10.7 Right to object according to Art. 21 GDPR ... 8
   10.8 Right to revoke consent declaration according to Art. 7 Para. 3 GDPR ... 8
   10.9 Right to complain to a supervisory authority according to Art. 77 GDPR ... 8
   10.10 Automated individual decision-making including profiling ... 9
11. d.velop cloud, cloud apps and On-Premises ... 9
   11.1 Operation of d.velop cloud, d.velop cloud apps and On-Premises ... 9
   11.2 Registration, ordering and license audits for d.velop cloud products ... 10
   11.3 d.velop documents ... 10
      11.3.1 Processing using deep learning ... 11
      11.3.2 Feedback form ... 11
   11.4 d.velop archivelink for SAP Solutions (SaaS) ... 12
   11.5 d.velop integration service for SAP Solutions ... 12
   11.6 d.velop sign ... 13

11.7 d.velop invoices 14
11.8 Evaluation of usage data for product optimisation 15
11.9 Additional services from third-party providers 16
11.9.1 HubSpot 16
11.9.2 Google Analytics 16
11.10 Information about the cookies we use 17
12. Employee apps 17
12.1 Community connect 17
12.2 Community chat 17
12.3 d.velop connect 18
12.4 d.velop care 18
12.5 Scope of data collection and processing 19
12.6 Legal basis for the processing of personal data in connection with our apps 19
12.7 Registration in our app 20
12.8 d.velop postbox 20
12.9 d.velop trust spaces 22
13. Data processing when using d.velop for Microsoft 365 products 23
13.1 Evaluation of login data for license audits 23
13.2 Monitoring the software status and reporting software errors 23
13.3 Audit logs ..... Error! Bookmark not defined.
13.4 Evaluation of usage data for product optimisation 25
13.5 Booking appointments with Microsoft Bookings 25

1. General information

1.1 Controller

We, d.velop AG, take your privacy and our legal obligations to protect your personal data very seriously. Legal regulations require us to be completely transparent in how we process your personal data. In order for you, as the data subject, to understand how we process your data, you need to be sufficiently informed about the necessity, purpose and scope of the processing. Our privacy policy therefore explains in detail which personal data we process when you use d.velop products and services. d.velop applications and services can be accessed through a website operated by d.velop or though an on-premises solution operated by you. You do not have to actively disclose any personal data to us to use this website. Nevertheless, we still process personal data when you simply visit our website. The privacy policy for our website can be found here. Within the meaning of the General Data Protection Regulation (GDPR), the Federal Data Protection Act (BDSG) and other data protection regulations, the "controller" for the processing listed here is:

d.velop AG
Schildarpstraße 6–8
48712 Gescher, Germany
+49 (0) 2542 9307-0
info@d-velop.de
www.d-velop.de
hereinafter referred to as "we," "us" or the "controller."

You can contact the data protection officer at:

Nils Möllers
Keyed GmbH
Siemensstrasse 12
48341 Altenberge, Germany
datenschutz@d-velop.de

This privacy policy applies to all companies of the d.velop Group. Certain products and services may also be offered by companies of the d.velop Group. Click here for a list of the d.velop Group companies.

As a rule, in providing the products and services offered, d.velop acts as processor in accordance with the data processing agreements concluded with you.

2. Definitions

2.1 Definitions from the GDPR

This privacy statement uses the terms defined in the legal text of the GDPR. These definitions (Art. 4 GDPR) can be found here.

2.2 Definitions for cookies and similar technologies

Cookies are text files that are stored or read on your device by a website or other service. They contain combinations of letters and numbers and are used to recognize the user and their settings when they reconnect to the website that set the cookie, to enable the user to remain logged in to a customer account, or to statistically analyze a specific user behavior.

Web Storage technology allows variables and values to be stored locally in the user's browser cache. This technology includes both "sessionStorage," which remains stored until the browser tab is closed, and "localStorage," which is stored in the browser cache until the user clears the cache. Among other things, the localStorage technology makes it possible to recognize the user and their settings when they open our services.

2.3 Definitions for data categories

When we specify in this privacy statement which categories of data we process, we are referring in particular to the following data:

- Master data (e.g. names, addresses, dates of birth)
- Contact details (e.g. e-mail addresses, phone numbers, messenger services)
- Content data (e.g. text entries, photographs, videos, contents of documents/files)
- Contract data (e.g. subject-matter of the agreement, terms, customer category)
- Payment data (e.g. bank details, payment history, use of other payment service providers)
- Usage data (e.g. history on our web services, use of certain content, access times)
- Connection data (e.g. device information, IP addresses, URL referrers)
- Location data (e.g. GPS data, IP geolocation, access points)

Most of our products and services involve data processing in some manner. In light of this and in accordance with the data processing agreements concluded with you, we as processor cannot conclusively define all the personal data that is processed, as it is the controller who defines the means and purposes of the processing.

3. Information about data processing

We process personal data only to the extent permitted by law. Personal data will be passed on to third parties only in the cases described below. Personal data is protected by appropriate technical and organizational measures (e.g. pseudonymization, encryption). Unless we are legally obliged to store or pass on personal data to third parties (in particular law enforcement agencies), the decision as to which personal data we process, how long we process it for and the extent to which we disclose it to others depends on which functions of the products you use in each individual case.

4. Legal basis for the processing of personal data

If we have obtained the data subject's consent to process their personal data, Art. 6 Para. 1 Lit. a) of the EU General Data Protection Regulation (GDPR) serves as the legal basis for the processing of this personal data.

If we are processing personal data that is necessary for the performance of a contract to which the data subject is a party, the legal basis is Art. 6 Para. 1 Lit. b) GDPR. This also applies to processing that is necessary to prepare a contract.

If processing of the personal data is necessary to fulfill a legal obligation to which our company is subject, the legal basis is Art. 6 Para. 1 Lit. c) GDPR.

In cases where the vital interests of the data subject or another natural person make it necessary to process personal data, the legal basis is Art. 6 Para. 1 Lit. d) GDPR.

If the processing is necessary to protect a legitimate interest of our company or a third party, and provided the interests, fundamental rights and freedoms of the data subject do not outweigh the aforementioned interest, the legal basis of the processing is Art. 6 Para. 1 Lit. f) GDPR.

The legal bases for your particular product and functions are listed below.

5. Duration of storage

Personal data shall be deleted as soon as the purpose for which it was processed no longer exits or a prescribed retention period expires, unless we need to continue storing the personal data in order to conclude or fulfill a contract.

6. Contact channels (support)

d.velop products contain contact forms or contact details that you can use to contact us electronically. If the data subject contacts our support through one of these channels, the personal data submitted by the data subject are saved automatically. These data are saved exclusively for the purpose of processing the request or

contacting the data subject. The data shall be deleted no later than three years from when the purpose of the processing ceases to apply. The data are not shared with third parties. For cases where the data subject's consent was obtained, the legal basis for the data processing is Art. 6, Para. 1, Lit. a) GDPR. The legal basis for processing data that were sent in an e-mail is Art. 6, Para. 1, Lit. f) GDPR. If the e-mail is sent with the aim of concluding a contract, the legal basis for the processing is also Art. 6 Para. 1 Lit. b) GDPR.

7. Social media login (signing up for a user account using a Facebook account)

Description and purpose: Users can sign up for an account using an existing Facebook account. When signing up with a Facebook account, the person who is authorized to access the Facebook account is authenticated. The provider then shares the data that you have agreed to disclose to sign up for the app, which in our case is your user name, e-mail address and, if applicable, a profile picture. Click here for information on Facebook account settings.

Legal basis: Consent, Art. 6, Para. 1, Lit. a) GDPR

Categories of data: User name, e-mail address, password, profile picture if applicable

Recipient(s) of the data: Facebook

Intended transfer to third countries: If necessary in individual cases under the responsibility of Facebook.

Storage duration: The data continues to be processed for as long as you use the social media login.

Revocation: Pursuant to Art. 7 Para. 3 Clause 1 of the GDPR, you have the right to revoke your consent at any time. This can be done informally and without the need to provide a reason; your revocation will apply to future processing only. Revoking your consent does not affect the lawfulness of processing carried out before the revocation. You can find further information in our privacy statement above, under "Rights of the data subject."

Legal or contractual obligation: You do not have any legal or contractual obligation to provide the data.

Does providing your consent mean that we store or read personal information on your device? No.

8. Proper use of our products and services, billing

In order to fulfill our contractual obligations and achieve our quality standards, it is essential that we process personal data. We therefore store and utilize technical logs containing usage and connection data in order to maintain and document the functionality of our products and services. This also constitutes our legitimate interest pursuant to Art. 6, Para. 1, Lit. f) GDPR.

Pursuant to Art. 6 Para. 1 Lit. b) or f) GDPR, we process personal data for the following purposes: to set up a customer account ("tenant") to enable use of d.velop products and the creation of additional users (e.g. employees); to process orders, including transaction e-mails; to record and collect your user ID and, if applicable, your e-mail address for license audits; and to ensure the security of our information technology systems. In these cases we process master data, contact details, usage data, connection data, contract data and payment data.

To ensure efficient processing we use Salesforce, a service operated by Salesforce.com Germany GmbH, Erika-Mann-Str. 31, 80636 Munich, Germany, and HubSpot, a service operated by HubSpot European Office, Ground Floor, Two Dockland Central Guild Street, Dublin 1, Ireland / HubSpot Inc., 25 First Street, 2nd Floor, Cambridge, MA 02141, USA. We ensure an appropriate level of security pursuant to the standard data protection clauses of the EU Commission, Art. 46 Para. 2 Lit. c) GDPR, and binding internal data protection rules, Art. 46 Para. 2 Lit. b) GDPR.

9. Ticket system

Description and purpose: We use the CRM and ticket system "Salesforce" of salesforce.com Germany GmbH, Erika-Mann-Str. 31, 80636 Munich. Salesforce is used to collect all inquiries from customers and interested parties in a uniform manner in order to be able to answer them more efficiently. Alternatively, you can also contact us by e-mail or telephone.

Legal basis: Art. 6 para. 1 letter f GDPR. Our legitimate interest lies in the proper processing of orders and transactions and the associated support.

Data categories: Master data, contact data, content data, usage data, connection data.

Recipient of the data: salesforce.com Germany GmbH, Erika-Mann-Str. 31, 80636 Munich, Germany.

Intended third country transfer: There will be no transfer of your personal data to a third country. However, we are aware of our responsibility and regularly review the framework conditions and legal changes.

Duration of data storage: The data is deleted as soon as it is no longer required to achieve the purpose for which it was collected. In addition, the data will be deleted if you exercise your right to erasure as defined in Article 17 (1) of the GDPR.

Objection: In the case of processing within the scope of legitimate interest, you have the right to object to the processing of your personal data at any time in accordance with Art. 21 (1) GDPR. If you exercise your right, processing for this purpose will no longer take place. Further information on this can be found above in our privacy policy under "Rights of data subjects".

Contractual or legal obligation: There is no contractual or legal obligation for the provision of the data.

Further data protection information: https://www.salesforce.com//company/privacy/

10. Rights of the data subject

If your personal data is processed, you are considered a data subject within the meaning of the GDPR and have the following rights vis-à-vis the controller:

10.1 Right of access according to Art. 15 GDPR

You have the right to ask the controller to confirm whether we are processing personal data about you. If we are processing such data, you may request information from the controller about the following:

a. For which purposes the personal data are processed
b. Which categories of personal data are processed
c. The recipients or categories of recipients to whom your personal data have been or will be disclosed
d. How long we plan to store your personal data or, if specific information cannot be provided, the criteria for determining the storage duration
e. Your right to rectification or erasure of your personal data, your right to restrict processing by the controller, and your right to object to such processing
f. Your right to appeal to a supervisory authority
g. All information available about the origin of the data, in the case that the personal data are not collected from the data subject themselves
h. Whether automated decision-making is used, including profiling pursuant to Art. 22 Para. 1 and 4 GDPR; in cases where such decision-making is used, you may also request meaningful information about the logic used and the scope and intended outcomes of said processing for the data subject

You have the right to request information about whether your personal data is transferred to a third country or to an international organization. In cases where such transfer takes place, you may request confirmation that appropriate safeguards are in place pursuant to Art. 46 GDPR.

10.2 Right to rectification according to Art. 16 GDPR

If your personal data are inaccurate or incomplete, you have the right to request that the controller rectify or complete the personal data. The controller shall rectify the data without undue delay.

10.3 Right to erasure according to Art. 17 GDPR

(1) You may request that the controller delete your personal data without undue delay, and the controller is obliged to delete such data without undue delay, if one of the following reasons applies:

a. The personal data concerning you is no longer necessary for the purposes for which it was collected or otherwise processed.
b. You withdraw your consent on which the processing was based pursuant to Art. 6 Para. 1 Lit. a) or Art. 9 Para. 2 Lit. a) GDPR and there is no other legal basis for the processing.
c. You object to the processing under Art. 21 Para. 1 GDPR and there are no overriding legitimate reasons for the processing, or you object to the processing under Art. 21 Para. 2 GDPR.
d. The personal data concerning you was processed unlawfully.
e. Deletion of the personal data concerning you is necessary to fulfil a legal obligation under European Union law or the law of the Member States to which the data controller is subject.
f. The personal data concerning you was collected in relation to information society services pursuant to Art. 8 Para. 1 GDPR.

(2) If the controller has disclosed your personal data and is obliged to delete it in accordance with Art. 17 Para. 1 GDPR, the controller shall, taking into account the available technology and costs of implementation, take appropriate measures, including technical measures, to inform other controllers who are processing this personal data that you, as data subject, have requested erasure of all links to or copies/replications of said personal data.

(3) Your right to erasure does not apply in cases where the processing is necessary for the following reasons:

a. To exercise the right to freedom of expression and information
b. To fulfil a legal obligation required by the law of the European Union or of the Member States to which the controller is subject, or to perform a task carried out in the public interest or in the exercise of official authority vested in the controller
c. For reasons of public interest in the field of public health pursuant to Art. 9 Para. 2 Lit. h) and i) and Art. 9 Para. 3 GDPR
d. For archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes pursuant to Art. 89 Para. 1 GDPR, insofar as the regulation referred to in Para. 1 presumably makes impossible or seriously impairs the attainment of the objectives of such processing
e. To assert, exercise or defend against legal claims

10.4 Right to restriction of processing according to Art. 18 GDPR

Under the following conditions, you can request that the processing of your personal data be restricted:

a. You dispute the accuracy of the personal data; in this case, processing will be restricted for a period of time that allows the controller to validate the personal data in question
b. The processing is unlawful and you refuse to delete the personal data and instead request that use of the personal data be restricted
c. The controller no longer needs the personal data for the purposes of the processing, but you need it to assert, exercise or defend against legal claims
d. You have lodged an objection against the processing pursuant to Art. 21 Para. 1 GDPR, and it has not yet been established that the controller's legitimate reasons outweigh yours

If the processing of your personal data has been restricted, these data may only be processed (excluding storage) with your consent, or for the purposes of asserting, exercising or defending against legal claims, or

to protect the rights of another natural or juridical person, or if the processing represents a compelling public interest of the Union or a Member State. If the processing has been restricted in accordance with the aforementioned conditions, you will be informed by the controller before the restriction is lifted.

10.5 Right of notification according to Art. 19 GDPR

If you have exercised your right to rectification, erasure or restriction of processing vis-à-vis the controller, the controller is obliged to notify all recipients to whom the personal data in question has been disclosed of this rectification or erasure of your personal data or the restriction of processing, unless such notification is impossible or is unreasonably burdensome. You have the right to be informed by the controller of the identifies of these recipients.

10.6 Right of data portability according to Art. 20 GDPR

You have the right to receive the personal data that you provided to the controller in a structured, common and machine-readable format. You also have the right to transfer these data to another controller without obstruction from the previous controller, provided that the following conditions are met:

a. The processing is based on consent pursuant to Art. 6 Para. 1 Lit. a) GDPR or Art. 9 Para. 2 Lit. a) GDPR, or based on a contract pursuant to Art. 6 Para. 1 Lit. b) GDPR
b. The data is processed using automated procedures. In exercising this right, you also have the right to request that your personal data be transmitted directly from one controller to another controller, as far as this is technically feasible. This must not impair the rights or freedoms of other persons. The right to data portability does not apply to data processing which is necessary to perform a task in the public interest or which is carried out in the exercise of official authority vested in the controller.

10.7 Right to object according to Art. 21 GDPR

You have the right to object at any time, on grounds relating to your particular situation, to processing of your personal data which is based on Art. 6 Para. 1 Lit. e) or f) GDPR; this also applies to any profiling based on these provisions. The controller will no longer process your personal data unless it can prove compelling reasons for processing which outweigh your interests, rights and freedoms, or the processing serves to assert, exercise or defend against legal claims. Where your personal data is processed for the purpose of direct marketing, you have the right to object at any time to the processing of your personal data for the purpose of such marketing; this also applies to profiling, to the extent that it is in connection with such direct marketing. If you object to processing for direct marketing purposes, your personal data will no longer be processed for these purposes. In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, you may exercise your right to object by automated means using technical specifications.

10.8 Right to revoke consent declaration according to Art. 7 Para. 3 GDPR

You have the right to revoke your declaration of consent to data processing at any time. Revoking your consent does not affect the lawfulness of processing carried out based on this consent before the revocation.

No specific form is required to lodge an objection or revoke consent. Such communications should be addressed to:

d.velop AG
Schildarpstraße 6–8
48712 Gescher, Germany
+49 (0) 2542 9307-0
info@d-velop.de

10.9 Right to complain to a supervisory authority according to Art. 77 GDPR

Without prejudice to any other administrative or judicial remedy, you have the right to lodge a complaint with a supervisory authority, in particular in the Member State in which you reside, work or where the alleged infringement took place, if you believe that the processing of your personal data infringes on the GDPR. The supervisory authority to which the complaint has been lodged shall inform the complainant of the status and

outcome of the complaint, including the possibility of a judicial remedy under Art. 77 GDPR. The responsible supervisory authority is:

Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen
Kavalleriestr. 2-4
40213 Düsseldorf, Germany
Phone: +49 (0) 211/38424-0
Fax: +49 (0) 211/38424-999
E-mail: poststelle@ldi.nrw.de

10.10 Automated individual decision-making including profiling

You have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects for you or otherwise has a significant impact on you. This does not apply if any of the following are true:

a. The decision is necessary for the conclusion or fulfillment of a contract between you and the controller
b. The decision is permitted by legislation of the Union or the Member States to which the controller is subject, and the legislation contains appropriate measures to safeguard your rights and freedoms and your legitimate interests
c. The decision is made with your express consent

However, these decisions must not be based on special categories of personal data pursuant to Art. 9 Para. 1 GDPR, unless Art. 9 Para. 2 Lit. a) or g) applies and appropriate measures have been taken to safeguard your rights, freedoms and legitimate interests.

For the cases referred to in points a. and c. above, the controller shall take reasonable steps to safeguard your rights, freedoms and legitimate interests, including at least the right to obtain human intervention on the part of the controller, to express your point of view and to contest the decision.

11. d.velop cloud, cloud apps and On-Premises

Using d.velop cloud and our apps requires the processing of personal data. We process data (especially pertaining to "users") as a processor pursuant to Art. 28 GDPR, for which we conclude a data processing agreement with the respective controller. Data processing of third-party apps is carried out within the scope of subcontracted processing. The main data processing company remains d.velop AG. Please also note the separate data protection information of the app providers.

11.1 Operation of d.velop cloud, d.velop cloud apps and On-Premises

Description and purpose: To store and utilize technical logs to ensure and demonstrate the functionality of our services and evaluation of anonymized usage data for product improvement. With d.velop cloud migration, documents and files can be migrated from a d.velop on-premises system to the d.velop cloud. The application builds on an export from the customer's on-premises source system, applies configured assignments of categories, properties, users and groups, takes into account further settings and then performs the migration to the cloud at the push of a button.

Legal basis: Art. 6, Para. 1, Lit. f) GDPR. It is in our legitimate interest to ensure trouble-free operation of the cloud and cloud apps and to document the functionality of the services as well as gaining insights into the use of our solutions so that we can continuously improve our products for our customers.

Categories of data: Usage data, connection data

Recipient(s) of the data: Data center/hosting providers

Intended transfer to third countries: None

Storage duration: Application logs: retained for as long as is technically necessary (e.g. a signature process log).

Infrastructure logs: up to 1 year (e.g. web server access logs)

Audit logs: up to 5 years (e.g. for logging changes to infrastructure or assigned permissions)

Backups: 30 days

In all other cases, the data are deleted as soon as they are no longer required to achieve the purpose for which they were collected. They are also deleted if you exercise your right to erasure as defined in Art. 17 Para. 1 GDPR.

Objection: In accordance with Art. 21 Para. 1 GDPR, you have the right to object to the processing of your personal data at any time. If you exercise your right, the data will no longer be processed for this purpose. You can find further information in our privacy statement above, under "Rights of the data subject."

Legal or contractual obligation: You do not have any legal or contractual obligation to provide the data.

11.2 Registration, ordering and license audits for d.velop cloud products

Description and purpose: To set up a customer account ("tenant") to enable use of d.velop cloud and the creation of additional users (e.g. employees); to process orders for d.velop cloud products, including transaction e-mails; to record and collect your user ID and, if applicable, your e-mail address for license audits; to ensure the security of our information technology systems.

Legal basis: Art. 6, Para. 1, Lit. b) and f) GDPR. In cases where Art. 6 Para. 1 Lit. f) GDPR is the legal basis, our legitimate interest lies in the proper provision of our products while also ensuring the security of our IT systems.

Categories of data: Master data, contact details, usage data, connection data, contract data, payment data

Recipient(s) of the data: Salesforce.com Germany GmbH, Erika-Mann-Str. 31, 80636 Munich, Germany; HubSpot European Office, Ground Floor, Two Dockland Central Guild Street, Dublin 1, Ireland / HubSpot Inc., 25 First Street, 2nd Floor, Cambridge, MA 02141, USA

Intended transfer to third countries: To the USA in individual cases (based on the standard data protection clauses of the EU Commission, Art. 46 Para. 2 Lit. c) GDPR and binding internal data protection rules, Art. 46 Para. 2 Lit. b) GDPR)

Storage duration: To document performance, we store license audit results until the retention period of 10 years expires.

Objection: For processing carried out in our legitimate interest, you have the right to object to the processing of your personal data at any time in accordance with Art. 21 Para. 1 GDPR. If you exercise your right, the data will no longer be processed for this purpose. You can find further information in our privacy statement above, under "Rights of the data subject."

Legal or contractual obligation: You do have legal or contractual obligation to provide the data.

11.3 d.velop documents

d.velop documents is the smart solution for accelerating, simplifying and optimizing the management of documents and information. Convenient digital filing and audit-proof storage enable customers to digitize their processes and work remotely. With d.velop documents, the customer can create fully integrated digital business processes from scanning to archiving, and enjoy the benefits of remote collaboration.

Further information about d.velop documents can be found in the corresponding product description.

11.3.1 Processing using deep learning

Description and purpose: Simplifies the handling of documents and their data as part of a digital document management concept. Documents are indexed using deep learning methods, e.g. to automatically determine document types, assign documents to storage locations, or detect key information. The information obtained is provided to you for easier processing.

Legal basis: Art. 6, Para. 1, Lit. f) GDPR. It is in our legitimate interest to provide you with this information to simply your processing.

Categories of data: master data, contact details, job title, payment data, license plate number.

Recipient(s) of the data: Amazon Web Services EMEA Sarl., 38 Avenue John F. Kennedy, L-1855, Luxembourg

Intended transfer to third countries: To the USA in individual cases (based on the standard data protection clauses of the EU Commission, Art. 46 Para. 2 Lit. c) GDPR)

Storage duration: We store the data for a maximum of 90 days.

Objection: For processing carried out in our legitimate interest, you have the right to object to the processing of your personal data at any time in accordance with Art. 21 Para. 1 GDPR. If you exercise your right, the data will no longer be processed for this purpose. You can find further information in our privacy statement above, under "Rights of the data subject."

Legal or contractual obligation: You do not have any legal or contractual obligation to provide the data.

11.3.2 Feedback form

Description and purpose: The form enables the user to share their opinion about the software in general, as well as suggestions for improvement or criticism. Feedback can be provided anonymously or from a specific user (user has the option to submit their name and e-mail address, which will then be stored). The following data are processed:

Legal basis: Art. 6, Para. 1, Lit. f) GDPR. It is in our legitimate interest to optimize the design of our product to meet our customers' needs and requests. Use of the feedback form is voluntary.

Categories of data:

- **Subject** is used to categorize the feedback.
- **Description** is needed to understand the user's praise/criticism/suggestions for improvement
- **Name** and **e-mail address** are required if the user wants us to contact them Entering the data is optional.
- User ID and tenant ID

Recipient(s) of the data: d.velop AG records the data in Salesforce and uses it internally for evaluation purposes.

Intended transfer to third countries: None

Storage duration: The data are deleted as soon as they are no longer required to achieve the purpose for which they were collected. The data are also deleted if you exercise your right to erasure as defined in Art. 17 Para. 1 GDPR.

Objection: For processing carried out in our legitimate interest, you have the right to object to the processing of your personal data at any time in accordance with Art. 21 Para. 1 GDPR. If you exercise your right, the data will no longer be processed for this purpose. You can find further information in our privacy statement above, under "Rights of the data subject."

Legal or contractual obligation: You do not have any legal or contractual obligation to provide the data.

11.4 d.velop archivelink for SAP Solutions (SaaS)

Description and purpose: d.velop archivelink for SAP Solutions is an interface that connects SAP systems such as SAP ERP ECC 6.0 or SAP S/4HANA (on premises) with d.velop documents. Audit-proof document storage is supported in all SAP storage scenarios specified by the SAP standard Archivelink interface. The user has the option to transmit document properties from the SAP system to the documents in d.velop documents.

For more information on d.velop archivelink for SAP Solutions (SaaS), please refer to the corresponding product description.

Legal basis: Art. 6, Para. 1, Lit. b) and f) GDPR. In cases where Art. 6 Para. 1 Lit. f) GDPR is the legal basis, our legitimate interest lies in the proper provision of our products while also ensuring the security of our IT systems.

Categories of data: With the d.velop archivelink for SAP Solutions interface, all data of SAP business objects that are relevant for document storage can be transferred to d.velop documents (e.g. master data of business partners, sales and purchase transactions, human resources master data, etc.).

Recipient(s) of the data: d.velop documents, data center/hosting providers

Intended transfer to third countries: To the USA in individual cases (based on the standard data protection clauses of the EU Commission, Art. 46 Para. 2 Lit. c) GDPR and binding internal data protection rules, Art. 46 Para. 2 Lit. b) GDPR).

Storage duration: The data are deleted as soon as they are no longer required to achieve the purpose for which they were collected. The data are also deleted if you exercise your right to erasure as defined in Art. 17 Para. 1 GDPR.

Objection: For processing carried out in our legitimate interest, you have the right to object to the processing of your personal data at any time in accordance with Art. 21 Para. 1 GDPR. If you exercise your right, the data will no longer be processed for this purpose. You can find further information in our privacy statement above, under "Rights of the data subject."

Legal or contractual obligation: You do not have any legal or contractual obligation to provide the data.

11.5 d.velop integration service for SAP Solutions

Description and purpose: d.velop integration service for SAP Solutions is an interface that connects SAP cloud systems such as SAP S/4HANA Public Cloud or SAP SuccessFactors with d.velop documents. Properties are read from the SAP systems and transferred to d.velop documents. Optionally, documents can be read from SAP SuccessFactors and stored in d.velop documents. Further information on d.velop integration service for SAP Solutions can be found in the corresponding service description.

Legal basis: Art. 6, Para. 1, Lit. b) and f) GDPR. In cases where Art. 6 Para. 1 Lit. f) GDPR is the legal basis, our legitimate interest lies in the proper provision of our products while also ensuring the security of our IT systems.

Data categories: With d.velop integration service for SAP Solutions, all data from relevant SAP business objects can be transferred to d.velop documents (e.g. master data from business partners, sales and purchasing transactions, personnel master data, etc.). Only key information necessary for processing is stored within the d.velop integration service for SAP Solutions. This data can be deleted automatically.

Recipients of the data: d.velop documents, providers of data centres/hosting

Intended transfer to third countries: In individual cases, the USA (based on the standard data protection clauses of the EU Commission, Art. 46 (2) (c) GDPR and binding internal data protection regulations, Art. 46 (2) (b) GDPR).

Duration of data storage: The data will be deleted as soon as it is no longer required for the purpose for which it was collected. In addition, the data will be deleted if you exercise your right to erasure within the meaning of Art. 17(1) GDPR.

Objection: In the case of processing within the scope of legitimate interest, you have the right to object to the processing of your personal data at any time in accordance with Art. 21(1) GDPR. If you exercise your right, processing for this purpose will no longer take place. Further information on this can be found above in our privacy policy under 'Rights of data subjects'.

Contractual or legal obligation: There is no contractual or legal obligation to provide the data.

11.6 d.velop sign

Description and purpose: d.velop sign is a signature app that enables you to provide qualified and legally compliant electronic signatures, in addition to simple and advanced signatures. This enables companies to legally sign contracts, invoices and other documents remotely (i.e. without additional hardware components). The procedure is recognized as legally valid within the EU in accordance with the eIDAS Regulation (Electronic Identification, Authentication and Trust Services).

The qualified signature fulfills the legal requirement of written form and is recognized by the courts. The advanced signature has a high probative value but is subject to a judge's discretion when considering evidence. The simple signature is unregulated, subject to a judge's discretion in considering evidence and does not require any identification. d.velop sign can be used immediately after purchase and works at the push of a button. Further information about d.velop sign can be found in the corresponding product description.

Legal basis: Art. 6, Para. 1, Lit. b) and f) GDPR. In cases where Art. 6 Para. 1 Lit. f) GDPR is the legal basis, our legitimate interest lies in the proper provision of our products while also ensuring the security of our IT systems.

Categories of data and recipient(s) of the data: We (d.velop sign) store the following information in the d.velop cloud (currently based on AWS and OTC, or data center service providers):

- d.velop sign/d.velop cloud user: Name und e-mail address (d.velop cloud)
- Billing address (d.velop cloud)
- Signature image (generated signature, freehand signature or uploaded signature image)

Data processed in d.velop sign:

- External users: e-mail address
    - Reporting for customer: evaluation of date, signature level, trustprovider, UserID and e-mail address (can only be seen by customer's admin)
- When signing with D-TRUST, the following data is entered in our screens during the first use and passed directly to D-TRUST (we do not store it):
    - Name
    - E-mail
    - Phone number
    - Password
    - Language

D-TRUST (sign-me) stores the aforementioned information on their HSMs.

For the advanced seal signature with Swisscom, only the user's e-mail address is required.

Document:

The document itself stays with d.velop (in the d.velop cloud) and only the document's hash value is transmitted to D-TRUST (sign-me).

When using the archive function in d.velop sign, documents can be archived from d.velop sign and data can be transferred to d.velop documents.

The integration of d.velop sign with d.velop documents enables documents to be transferred between d.velop documents and d.velop sign.

Intended transfer to third countries: To the USA in individual cases (based on the standard data protection clauses of the EU Commission, Art. 46 Para. 2 Lit. c) GDPR and binding internal data protection rules, Art. 46 Para. 2 Lit. b) GDPR). d.velop sign uses only services based in Germany.

Storage duration: The data are deleted as soon as they are no longer required to achieve the purpose for which they were collected. The data are also deleted if you exercise your right to erasure as defined in Art. 17 Para. 1 GDPR. Documents stored in d.velop sign are retained for the following durations:

If documents are not actively deleted:

- The documents are automatically deleted after 12 months.

If documents are deleted by the user:

- When documents are actively deleted, the documents are initially deleted only logically (can no longer be searched).
- The documents are then physically deleted after 30 days.

If documents are archived by the user:

- Documents can be archived in a connected d.velop documents application to prevent automatic deletion and to keep the documents for a longer period.

Objection: For processing carried out in our legitimate interest, you have the right to object to the processing of your personal data at any time in accordance with Art. 21 Para. 1 GDPR. If you exercise your right, the data will no longer be processed for this purpose. You can find further information in our privacy statement above, under "Rights of the data subject."

Legal or contractual obligation: You do not have any legal or contractual obligation to provide the data.

11.7 d.velop invoices

Description and purpose: d.velop invoices is the smart solution for accelerating, simplifying and optimizing the processing of invoice documents. Convenient digital filing and audit-proof storage enable customers to digitize their processes and work remotely. With d.velop invoices, the customer can create fully integrated digital business processes, from import to workflows to archiving, and enjoy the benefits of remote collaboration. Further information about d.velop invoices can be found in the corresponding product description.

Legal basis: Art. 6, Para. 1, Lit. b) and f) GDPR. In cases where Art. 6 Para. 1 Lit. f) GDPR is the legal basis, our legitimate interest lies in the proper provision of our products while also ensuring the security of our IT systems.

Categories of data: Master data, contact details, usage data, connection data, contract data, payment data

Recipient(s) of the data:

- Amazon Web Services
- Microsoft Azure
- d.velop (processing of contact details and contract data)
- Grafana (for evaluation purposes)

Intended transfer to third countries: To the USA in individual cases (based on the standard data protection clauses of the EU Commission, Art. 46 Para. 2 Lit. c) GDPR and binding internal data protection rules, Art. 46 Para. 2 Lit. b) GDPR).

Storage duration: The data are deleted as soon as they are no longer required to achieve the purpose for which they were collected. The data are also deleted if you exercise your right to erasure as defined in Art. 17 Para. 1 GDPR.

Objection: For processing carried out in our legitimate interest, you have the right to object to the processing of your personal data at any time in accordance with Art. 21 Para. 1 GDPR. If you exercise your right, the data will no longer be processed for this purpose. You can find further information in our privacy statement above, under "Rights of the data subject."

Legal or contractual obligation: You do not have any legal or contractual obligation to provide the data.

11.8 Analysis of Technical Log Data to Ensure Operations
Description and Purpose

When using the d.velop Cloud and our apps, technical log data is generated automatically. This includes, among other things, web server access logs, application runtime logs, and infrastructure logs from the cloud or hyperscaler environments in use. These logs may contain personal data such as IP addresses or usernames.

The processing of this log data is carried out to ensure technical operations, and in particular for the following purposes:

- Error handling and fault analysis during ongoing operation of the service offering
- Monitoring of performance, availability, and IT security, including SIEM
- Traceability of technical events in the context of IT forensics
- Alerting in the event of service disruptions, outages, or security-related anomalies

In accordance with the service description, this log data is encrypted both during transmission (in transit) and at rest.

Alerts based on log data, for example to verify service disruptions, outages, or security-related anomalies, are forwarded to an on-call solution. The handling, preparation, and root cause analysis of incidents (incident response) also take place within this on-call solution.

Legal Basis: Art. 6 (1) (f) GDPR. Our legitimate interest lies in ensuring the uninterrupted operation of the Cloud and Cloud Apps, in demonstrating the functionality of the services, and in gaining insights into the use of our solutions so that we can continuously improve our products for our customers.

Data Categories: Technical log data, connection data

Data Processing and Processing Location: The processing of log data takes place primarily on the infrastructure of T-Systems International GmbH / T Cloud Public:

T-Systems International GmbH
Hahnstraße 43d
60528 Frankfurt am Main

The analysis of security-related events (SIEM) is carried out by d.velop employees on their own infrastructure. The operation (including patch management and operating system configuration) of the SIEM software required for this purpose is supported by SVA:

SVA System Vertrieb Alexander GmbH
Borsigstraße 26
65205 Wiesbaden

In the event of alerts, excerpts of the logs are processed in the on-call solution incidents.io:

Pineapple Technology Ltd (incident.io)
66 City Road
EC1Y 2AL London

Data Retention Period: The data will be deleted as soon as it is no longer necessary for the purpose for which it was collected.

Objection: In the case of processing based on legitimate interest, you have the right at any time to object to the processing of your personal data pursuant to Art. 21(1) GDPR. If you exercise this right, processing for this purpose will no longer take place. For further information, please refer to the section "Rights of Data Subjects" above in our privacy policy.

11.9 Additional services from third-party providers

11.9.1 HubSpot

Description and purpose: E-mail tracking exclusively for transaction e-mails to ensure proper handling of transactions for orders of d.velop cloud products.

Legal basis: Art. 6, Para. 1, Lit. f) GDPR. It is in our legitimate interest to ensure the proper processing of orders and transactions in d.velop cloud products.

Categories of data: Master data, contact details, content data, usage data, connection data

Recipient(s) of the data: HubSpot European Office, Ground Floor, Two Dockland Central Guild Street, Dublin 1, Ireland / HubSpot Inc., 25 First Street, 2nd Floor, Cambridge, MA 02141, USA

Intended transfer to third countries: To the USA in individual cases (based on the standard data protection clauses of the EU Commission, Art. 46 Para. 2 Lit. c) GDPR)

Storage duration: The data are deleted as soon as they are no longer required to achieve the purpose for which they were collected. The data are also deleted if you exercise your right to erasure as defined in Art. 17 Para. 1 GDPR.

Objection: For processing carried out in our legitimate interest, you have the right to object to the processing of your personal data at any time in accordance with Art. 21 Para. 1 GDPR. If you exercise your right, the data will no longer be processed for this purpose. You can find further information in our privacy statement above, under “Rights of the data subject.”

Legal or contractual obligation: You do not have any legal or contractual obligation to provide the data.

Does providing your consent mean that we store or read information on your device? Yes.

Further privacy information: here

11.9.2 Google Analytics

Description and purpose: Statistical evaluation of how you use the d.velop cloud platform. We collect your IP address before it is anonymized by Google through truncation before being permanently stored on their servers.

Legal basis: Art. 6, Para. 1, Lit. a) GDPR

Categories of data: Usage data, connection data

Recipient(s) of the data: Google Ireland Ltd., Gordon House, Barrow Street Dublin 4 Ireland

Intended transfer to third countries: To the USA in individual cases (based on the standard data protection clauses of the EU Commission, Art. 46 Para. 2 Lit. c) GDPR)

Storage duration: The data are deleted as soon as they are no longer required to achieve the purpose for which they were collected. The data are also deleted if you exercise your right to erasure as defined in Art. 17 Para. 1 GDPR.

Revocation: Pursuant to Art. 7 Para. 3 Clause 1 of the GDPR, you have the right to revoke your consent at any time. This can be done informally and without the need to provide a reason; your revocation will apply to future processing only. Revoking your consent does not affect the lawfulness of processing carried out before the revocation. You can find further information in our privacy statement above, under "Rights of the data subject."

Legal or contractual obligation: You do not have any legal or contractual obligation to provide the data.

Does providing your consent mean that we store or read information on your device? Yes.

Further privacy information: Click here for further information about terms of use and data protection.

11.10 Information about the cookies we use

Below is a list of the names and functional durations of the cookies used by the above mentioned plugins and services – provided you consent to their use – with the following pattern:

[name of the service]: [name of the cookie] ([functional duration]).

A cookie can only be accessed from the Internet address at which the cookie was set. This means that we have no access to the cookies used by the other providers (above). They also have no access to our cookies. Third parties have access neither to our cookies nor to those of the other providers. Third parties can only access these cookies by means of technical attacks, which we cannot control and for which we are not responsible.

Google Analytics: _ga (2 years), _gid (2 years)

Userlane: userlane-user (5 years)

HubSpot: __hs_opt_out, __hs_do_not_track, hs_ab_test, _key, hs-messages-is-open, hs-messages-hide-welcome-message, __hsmem, messagesUtk (13 months)

12. Employee apps

12.1 Community connect

d.velop AG provides a platform (hereinafter also referred to as the "d.velop community connect app") for disseminating information.

The d.velop community connect app lets you make information available to all stakeholders, regardless of time and place. It serves as a central, mobile and digital touchpoint for organizational communication.

Further information about community connect can be found in the corresponding product description.

12.2 Community chat

d.velop AG provides a platform (hereinafter also referred to as "d.velop community chat") on which users can chat with each other.

With d.velop community chat, customers can send and receive messages and transfer documents, images and videos to other users in all file formats. Each user must be a member of the platform.

Admins with access to the database can also view the following data:

- PSUID (unique user ID)
- Rooms entered
- Invitations sent
- Rooms created
- Public rooms entered
- Information about who the user chats with in private rooms
- Files uploaded to the channel (can be encrypted)

Further information about community chat can be found in the corresponding product description.

12.3 d.velop connect

Description and purpose: d.velop connect supports internal and external communication and collaboration. With the first version, it will be possible to distribute information (content such as blogs or news, checklists and events, as well as a user directory) to employees in the company and external users and to receive feedback on the information via "reactions" (emojis and comments). Location-independent access to relevant information and documents via mobile apps (Android and iOS) plays a central role here.

Administration and editing can be carried out for authorized accounts via a special web interface. In addition, editorial content can also be created and edited via the mobile apps.

Legal basis: The legal basis for the processing of your personal data is Art. 6 para. 1 lit. a), b) GDPR.

Recipient(s) of the data: The recipient of your personal data is d.velop AG, Schildarpstrasse 6-8, 48712 Gescher, Germany, as well as Open Telekom Cloud (hosting), Cidaas (identity provider) and twilio Send-grid (e-mail dispatch).

Intended transfer to third countries: Personal data is transferred to the USA. The transfer is subject to suitable guarantees in accordance with Art. 46 GDPR. We have concluded standard contractual clauses with the data importer for this purpose. In addition, we are aware of our responsibility and, where necessary, take further measures to protect the rights and freedoms of natural persons to ensure the protection of personal data.

Storage duration: The data is deleted as soon as it is no longer required to achieve the purpose for which it was collected. In addition, the data will be deleted if you assert your right to deletion within the meaning of Art. 17 para. 1 GDPR.

Revocation: You have the right to withdraw your consent at any time, see Art. 7 para. 3 sentence 1 GDPR. This can be done informally and without giving reasons and is effective for the future. The withdrawal of consent does not affect the lawfulness of the processing carried out prior to the withdrawal. Further information on this can be found above in our privacy policy under "Rights of data subjects".

Legal or contractual obligation: There is no contractual or legal obligation to provide the data.

Further privacy information: Further information on the processing of your personal data can be found here: https://www.d-velop.com/privacy-policy

12.4 d.velop care

Description and purpose: d.velop care is a communication platform for social work providers, associations and institutions that helps users to design communication processes – both internal and with clients – that comply with data protection regulations. Communication processes can be designed using chats, appointment scheduling tools and functions for sharing information and documents relating to the collaboration.

Further information about d.velop care can be found in the corresponding product description.

Legal basis: Art. 6, Para. 1, Lit. b) and f) GDPR. In cases where Art. 6 Para. 1 Lit. f) GDPR is the legal basis, our legitimate interest lies in the proper provision of our products while also ensuring the security of our IT systems.

Categories of data: Master data, contact details, usage data, connection data, contract data, payment data

Recipient(s) of the data: Data center/hosting providers

Intended transfer to third countries: None

Storage duration: The data are deleted as soon as they are no longer required to achieve the purpose for which they were collected. The data are also deleted if you exercise your right to erasure as defined in Art. 17 Para. 1 GDPR.

Objection: For processing carried out in our legitimate interest, you have the right to object to the processing of your personal data at any time in accordance with Art. 21 Para. 1 GDPR. If you exercise your right, the data will no longer be processed for this purpose. You can find further information in our privacy statement above, under "Rights of the data subject."

Legal or contractual obligation: You do not have any legal or contractual obligation to provide the data.

12.5 Scope of data collection and processing

Unless otherwise stated in the following sections, we generally collect, process or use your personal data when you use our apps in order to meet our quality standards. During registration, we first collect the user's master data:

- First and last name
- Language and country/region
- e-mail address

Additional personal data is collected when using the apps in order to enable trustworthy connections between users within the apps. We may collect the following additional data:

- Contact details
- Professional status
- Profile pictures

We also use web-based structures to gather certain technical information based on the data transmitted by your browser (for example, browser type/version, operating system used). We may collect the following data:

- Information about your browser type and version
- User's operating system
- Device ID
- User's IP address
- Date and time of access
- Which web pages the user's system accessed via our app, if additional data must be obtained from the community connect server

12.6 Legal basis for the processing of personal data in connection with our apps

In accordance with and in fulfillment of our contract, we process your personal data for the following purposes pursuant to Art. 6 Para. 1 Lit. b) GDPR:

- To provide you with the apps and related services
- To notify you about changes to our services
- To provide you with user support
- To enforce our terms, conditions and policies
- To manage the apps, including troubleshooting

- To allow you to share user content with other users and interact with them

In order to provide effective and dynamic apps in pursuance of our legitimate interests in accordance with Art. 6 Para. 1 Lit. f) GDPR, we may use your data for the following:

- To ensure your safety and security, including reviewing user content, messages, and related metadata for violations of our community policies and our terms of use
- To ensure that content is presented in the most effective way for you and your device
- To understand how users use the apps so that we can improve, promote and further develop them
- To verify your identity, for example to grant you a verified account, and to verify your age, for example to ensure that you are old enough to use certain features
- To provide non-personalized advertising via business profiles so that we can keep many of our services free

When we process your data in fulfillment of our legitimate interests, we conduct an appropriateness review to determine whether the use of personal data is truly necessary to achieve our business purpose. When we conduct this review, we also consider our users' privacy rights and take appropriate precautions to protect their personal information.

If we have obtained the data subject's consent to process their personal data, Art. 6 Para. 1 Lit. a) of the EU General Data Protection Regulation (GDPR) serves as the legal basis for the processing of this personal data. If we are processing personal data that is necessary for the performance of a contract to which the data subject is a party, the legal basis is Art. 6 Para. 1 Lit. b) GDPR. This also applies to processing that is necessary to prepare a contract. If processing of the personal data is necessary to fulfill a legal obligation to which our company is subject, the legal basis is Art. 6 Para. 1 Lit. c) GDPR. In cases where the vital interests of the data subject or another natural person make it necessary to process personal data, the legal basis is Art. 6 Para. 1 Lit. d) GDPR. If the processing is necessary to protect a legitimate interest of our company or a third party, and provided the interests, fundamental rights and freedoms of the data subject do not outweigh the aforementioned interest, the legal basis of the processing is Art. 6 Para. 1 Lit. f) GDPR.

12.7 Registration in our app

If the data subject exercises the option in d.velop postbox to sign up for the controller's app by providing personal data, the data entered in the form will be transmitted to the controller. This data is stored exclusively for internal use by the controller. The data are deleted as soon as they are no longer required to achieve the purpose for which they were collected. During registration, the user's IP address and the date and time of registration are stored (d.velop postbox). This prevents misuse of the services. The data are not shared with third parties. The only exception is cases where there is a legal obligation to disclose the data. Registration of the data is necessary to provide content or services. Registered persons can have their stored data deleted or modified at any time. The data subject can obtain information about their stored personal data at any time.

12.8 d.velop postbox

Description and purpose: d.velop postbox is a digital mailbox. The user can use the platform to receive and send digital documents to registered companies and organizations in compliance with legal regulations. The documents become the property of the user and can be accessed using a web browser or the smartphone apps offered for iOS and Android.

Further information about d.velop postbox can be found in the corresponding product description.

Legal basis: Art. 6, Para. 1, Lit. b) and f) GDPR. In cases where Art. 6 Para. 1 Lit. f) GDPR is the legal basis, our legitimate interest lies in the proper provision of our products while also ensuring the security of our IT systems.

Categories of data: The data collected can be divided into the following categories:

- User data (user name, e-mail, also name and address, if provided (optional))

- Log files (user ID, anonymized IP address)
- Provider data (contact details for fulfillment of the contract)
- E-mail data (originating from d.velop postbox, for notifying the user)
- Usage data (for analyzing user behavior)

Recipient(s) of the data: d.velop postbox, data center/hosting providers

Intended transfer to third countries: Your personal data are not transferred to third countries. However, we take our responsibility seriously and regularly review the situation and any changes to the legal landscape. In the event that your data is indeed transferred to a third country, we will adapt this information as quickly as possible.

Storage duration: The duration of data storage depends on the aforementioned data categories as follows:

- User data: until the user account is deleted plus a maximum of 48 hours in which to object to the deletion
- Log files: 30 days after collection
- Provider data: 3 years after termination of the contractual relationship
- E-mail data: 30 days after collection
- Usage data: not deleted until purpose is achieved. Unless the right to erasure is exercised within the meaning of Art. 17 Para. 1 GDPR

Objection: For processing carried out in our legitimate interest, you have the right to object to the processing of your personal data at any time in accordance with Art. 21 Para. 1 GDPR. If you exercise your right, the data will no longer be processed for this purpose. You can find further information in our privacy statement above, under "Rights of the data subject."

Legal or contractual obligation: You do not have any legal or contractual obligation to provide the data.

12.9 Analysis of Technical Log Data to Ensure Operations

Description and Purpose: When using d.velop postbox, technical log data is generated automatically. This includes, among other things, web server access logs, application runtime logs, and infrastructure logs from the cloud or hyperscaler environments in use. These logs may contain personal data, as well as log files (user ID, anonymised IP address).

The processing of this log data is carried out to ensure technical operations, and in particular for the following purposes:

- Error handling and fault analysis during ongoing operation of the service offering
- Monitoring of performance, availability, and IT security, including SIEM
- Traceability of technical events in the context of IT forensics
- Alerting in the event of service disruptions, outages, or security-related anomalies

In accordance with the service description, this log data is encrypted both during transmission (in transit) and at rest.

Legal Basis: Art. 6 (1) (f) GDPR. Our legitimate interest lies in ensuring the uninterrupted operation of the Cloud and Cloud Apps, in demonstrating the functionality of the services, and in gaining insights into the use of our solutions so that we can continuously improve our products for our customers.

Data Categories: Technical log data, connection data

Data Processing and Processing Location: The analysis of security-related events (SIEM) is carried out by d.velop employees on their own infrastructure. The operation (including patch management and operating system configuration) of the SIEM software required for this purpose is supported by SVA:

SVA System Vertrieb Alexander GmbH
Borsigstraße 26
65205 Wiesbaden

Data Retention Period: The data will be deleted as soon as it is no longer necessary for the purpose for which it was collected.

Objection: In the case of processing based on legitimate interest, you have the right at any time to object to the processing of your personal data pursuant to Art. 21(1) GDPR. If you exercise this right, processing for this purpose will no longer take place. For further information, please refer to the section "Rights of Data Subjects" above in our privacy policy.

12.10 d.velop trust spaces

Description and purpose: d.velop trust spaces enables the administration and sending of shared documents and data. This is to enable cross-organizational, collaborative cooperation. In addition, for the purpose of product improvement, user behavior is evaluated anonymously within trust spaces. The evaluation does not allow any conclusions to be drawn about the person concerned.

For further information on d.velop trust spaces, please refer to the associated product description.

Legal basis: Art. 6 para. 1 letters a, b, f GDPR. In cases where Art. 6 (1) letter f GDPR is the relevant legal basis, our legitimate interest lies in the proper provision of our products while ensuring the security of our IT systems.

Data categories: The collected data can be divided into the following categories: Contact data, master data, content data, usage data, connection data, diagnostic data data of the website/app, other technical data for the analysis of malfunctions and errors).

Recipients of the data: d.velop, data center/hosting provider, provider for the provision of the login area.

Intended third country transfer: there is no transfer of your personal data to a third country. However, we are aware of our responsibility and regularly review the framework conditions and legal changes.

Duration of data storage: The data is deleted as soon as it is no longer required to achieve the purpose for which it was collected. In addition, the data will be deleted if you exercise your right to erasure as defined in Article 17 (1) of the GDPR. In addition, below you will find the names and functional duration of the cookies used by the above-mentioned plugins and services - in case of their consent - according to the scheme [name of the service]: [name of the cookie] ([function duration]).

- d.velop trust spaces repository
    - RepoSession (24 hours, user login)
    - RepoSelectedSpace (1 year, On exit of browser session, information about the last selected space)
    - LastSeenArticles (1 year, information about last seen new articles)
- d.velop trust spaces identity
    - IdentitySession (24 hours, user login)
- Cidaas
    - cidaas_dr (1 year, user login)
    - cidaas_rl (unlimited, user login)
    - cidaas_sid (1 year, user login)

- cidaas_sso (1 year, user login)

Revocation and objection: You have the right to revoke your consent at any time, cf. Art. 7 para. 3 p. 1 GDPR. This can be done informally and without giving reasons and is effective for the future. The revocation of consent does not affect the lawfulness of the processing carried out until the revocation. Further information on this can be found in our data protection declaration under "Rights of the data subjects". In the case of processing within the scope of legitimate interest, you have the right to object to the processing of your personal data at any time in accordance with Article 21 (1) of the GDPR. If you exercise your right, processing for this purpose will no longer take place. Further information on this can be found above in our privacy policy under "Rights of data subjects".

Contractual or legal obligation: There is no contractual or legal obligation for the provision of the data.

13. Data processing when using d.velop for Microsoft 365 products

Your use of d.velop for Microsoft 365 products and their functions requires us to regularly process certain personal data. For use of d.velop for Microsoft 365 products, we are the controller for the processing listed below within the meaning of the General Data Protection Regulation (GDPR), the Federal Data Protection Act (BDSG) and other data protection regulations. Furthermore, we also process data as a processor pursuant to Art. 28 GDPR, for which we conclude a data processing agreement with the respective controller.

13.1 Evaluation of login data for license audits

Description and purpose: We collect and record your user ID and possibly your e-mail address in order to conduct license audits.

Legal basis: Art. 6, Para. 1, Lit. f) GDPR. It is in our legitimate interest to ensure the proper billing of our services and licenses.

Categories of data: Contact details, connection data

Recipient(s) of the data: None

Intended transfer to third countries: None

Storage duration: The data are deleted as soon as they are no longer required to achieve the purpose for which they were collected. The data are also deleted if you exercise your right to erasure as defined in Art. 17 Para. 1 GDPR.

Objection: For processing carried out in our legitimate interest, you have the right to object to the processing of your personal data at any time in accordance with Art. 21 Para. 1 GDPR. If you exercise your right, the data will no longer be processed for this purpose. You can find further information in our privacy statement above, under “Rights of the data subject.”

Legal or contractual obligation: You do not have any legal or contractual obligation to provide the data.

Does providing your consent mean that we store or read personal information on your device? No

13.2 Monitoring the software status and reporting software errors

Description and purpose: As a customer of d.velop, you can register with Statuspal to monitor the availability of d.velop for Microsoft 365 products and to be notified about software errors and maintenance work. Statuspal will then contact you directly. Statuspal does not act as a processor for d.velop. Click here for information about data processing by Statuspal.

Legal basis: Art. 6, Para. 1, Lit. b) and f) GDPR. It is in our legitimate interest to maintain our quality standards in terms of the availability of our solutions and our communication with our customers.

Categories of data: Contact details

Recipient(s) of the data: Statuspal, E.M. Statuspal UG, Strassmannstrasse 8, 10249 Berlin. If you register with Statuspal: communication service providers (Twitter, Slack, e-mail providers)

Storage duration: Since you register directly with the provider, we do not store any personal data about you. Click here for information about Statuspal's privacy policy.

Objection: For processing carried out in our legitimate interest, you have the right to object to the processing of your personal data at any time in accordance with Art. 21 Para. 1 GDPR. If you exercise your right, the data will no longer be processed for this purpose. You can find further information in our privacy statement above, under "Rights of the data subject."

Legal or contractual obligation: You do not have any legal or contractual obligation to provide the data.

13.3 Analysis of Technical Log Data to Ensure Operations

Description and Purpose: When using the d.velop Cloud and our apps, technical log data is generated automatically. This includes, among other things, web server access logs, application runtime logs, and infrastructure logs from the cloud or hyperscaler environments in use. These logs may contain personal data such as IP addresses or usernames.

The processing of this log data is carried out to ensure technical operations, and in particular for the following purposes:

- Error handling and fault analysis during ongoing operation of the service offering
- Monitoring of performance, availability, and IT security, including SIEM
- Traceability of technical events in the context of IT forensics
- Alerting in the event of service disruptions, outages, or security-related anomalies

In accordance with the service description, this log data is encrypted both during transmission (in transit) and at rest.

Alerts based on log data, for example to verify service disruptions, outages, or security-related anomalies, are forwarded to an on-call solution. The handling, preparation, and root cause analysis of incidents (incident response) also take place within this on-call solution.

Legal Basis: Art. 6 (1) (f) GDPR. Our legitimate interest lies in ensuring the uninterrupted operation of the Cloud and Cloud Apps, in demonstrating the functionality of the services, and in gaining insights into the use of our solutions so that we can continuously improve our products for our customers.

Data Categories: Technical log data, connection data

Data Processing and Processing Location: The processing of log data takes place primarily on the infrastructure of T-Systems International GmbH / T Cloud Public:

T-Systems International GmbH
Hahnstraße 43d
60528 Frankfurt am Main

The analysis of security-related events (SIEM) is carried out by d.velop employees on their own infrastructure. The operation (including patch management and operating system configuration) of the SIEM software required for this purpose is supported by SVA:

SVA System Vertrieb Alexander GmbH
Borsigstraße 26
65205 Wiesbaden

In the event of alerts, excerpts of the logs are processed in the on-call solution incidents.io:

Pineapple Technology Ltd (incident.io)
66 City Road
EC1Y 2AL London

Data Retention Period: The data will be deleted as soon as it is no longer necessary for the purpose for which it was collected.

Objection: In the case of processing based on legitimate interest, you have the right at any time to object to the processing of your personal data pursuant to Art. 21(1) GDPR. If you exercise this right, processing for this purpose will no longer take place. For further information, please refer to the section "Rights of Data Subjects" above in our privacy policy.

13.4 Evaluation of usage data for product optimisation

Description and purpose: As part of the continuous development and optimisation of our products, we analyse anonymised usage data. The aim of this evaluation is to improve the functionality and user-friendliness of our solutions in a targeted manner. The term 'usage data' includes, for example, user interactions such as filing a delivery note document. No content data such as the content or name of the filed document is recorded. The data is collected using the provided user ID, which is anonymised using cryptographic methods selected in accordance with current security standards and supplementary technical and organisational measures.

Legal basis: Art. 6 (1) (f) GDPR. Our legitimate interest lies in the further optimisation of our products in order to be able to provide customers with optimised products.

Categories of data: Usage data, connection data

Recipients of the data: None

Intended transfer to third countries: None

Duration of data storage: The data is not personal data, as it is anonymised accordingly. The data is deleted as soon as it is no longer required for the purpose for which it was collected.

Objection: In the case of processing within the scope of legitimate interest, you have the right to object to the processing of your personal data at any time in accordance with Art. 21 (1). If you exercise your right, processing for this purpose will no longer take place. Further information on this can be found above in our privacy policy under 'Rights of data subjects'.

Contractual or legal obligation: There is no contractual or legal obligation to provide the data.

13.5 Booking appointments with Microsoft Bookings

Description and purpose: We use Microsoft Bookings to create and manage appointments. Microsoft Bookings simplifies and speeds up these processes. The person concerned (customer/interested party/third party) can independently choose between different subject areas and thus arrange an appointment with a suitable contact person.

Legal basis: Art. 6 para. 1 letter f GDPR. Our legitimate interest lies in enabling quick and easy appointment coordination.

Data categories: Contact details

Recipients of the data: None

Intended third country transfer: Through the use of the service, personal data may be transferred to a third country. In the event of a transfer of personal data, the Provider shall ensure the level of protection of the GDPR by complying with Art. 44 et seq. GDPR. If there is no adequacy decision with the third country in which the data importer is based, the transfer is subject to appropriate guarantees. If you have any questions, please contact our data protection officer.

Duration of data storage: The data is deleted as soon as it is no longer required to achieve the purpose for which it was collected. In addition, the data will be deleted if you assert your right to deletion as defined in Article 17 (1) of the GDPR.

Objection: In the case of processing in the context of legitimate interest, you have the right to object to the processing of your personal data at any time in accordance with Art. 21 (1). If you exercise your right, processing for this purpose will no longer take place. Further information on this can be found above in our data protection declaration under "Rights of data subjects".

Contractual or legal obligation: There is no contractual or legal obligation to provide the data.

Further information on data protection: https://privacy.microsoft.com/de-de/privacystatement