Privacy policy for the Device as a Service activities

This privacy policy applies to the processing of personal data within the framework of our Device as a Service activities (it is also referred to as "DaaS" or "DaaS products and/or services" in this privacy policy). We have drafted this privacy policy in an easy to understand way to help you learn who we are, which personal data we collect about you, why we collect this data and what we do with this data. We also inform you in this privacy policy about the rights that you have.

Bear in mind that personal data (also referred to as "data" or "your data" in this privacy policy) comprises all information or information sets with which we can personally identify you directly or indirectly, in particular based on an identifying reference such as first and last names, email address or telephone number, but also your IP address, for example.

We take the protection of your personal data seriously. This means, for example, that we process your data in accordance with the applicable legislation for the protection of personal data, in particular the EU General Data Protection Regulation (EU GDPR).

We strongly recommend that you take your time to read this privacy policy. Please do not give us personal data if you do not agree with this privacy policy.

Scope of application

This privacy policy explains how we collect, store, issue and/or use in another way your data when you show interest in our DaaS products and/or services.

This privacy policy only applies to our DaaS products and/or services that we provide to business customers (B2B).

Rights of the data subject

Firstly, we want to inform you about your rights as a data subject. This is set down in articles 15 to 22 of the EU GDPR and comprises:

- The right of access by the data subject (article 15 of the EU GDPR);
- The right to erasure ("right to be forgotten") (article 17 of the EU GDPR);
- The right to rectification (article 16 of the EU GDPR);
- The right to data portability (article 20 of the EU GDPR);
- The right to restrict processing (article 18 of the EU GDPR);
- The right to object (article 21 of the EU GDPR).

If you wish to exercise your rights, please contact the Centre of Excellence (hereinafter to be referred to as the: 'CoE') using the following email address: mcoe@bechtle.com**.**

Right to object: In relation to your right to object, please remember that if we process personal data for mailings, you always have the right to object to this data processing without giving a reason. This also applies to profiling to the extent that this is related to mailings.

If you object to the processing in relation to mailings, we will no longer process your personal data for this purpose.You can object free of charge and it does not have to be done in a specific

format.We would prefer that you address your objection to the CoE using the following email address: mcoe@bechtle.com**.**

Should we process your data in order to pursue legitimate objectives, you can always object to this processing for special personal reasons. This also applies to profiling based on these provisions. We will then stop processing your personal data unless we can prove that we have urgent legitimate reasons for the processing that prevail above your interests, rights and freedoms or unless the processing is to determine, exercise or defend legal actions.

Types of data subjects

Within the framework of our services, we may collect personal data with regard to:

- Our B2B customers, other contract parties and potential customers insofar as they are active as independent entrepreneurs or general partnerships (in which case the data that is related directly or indirectly with these parties is regarded as personal data in accordance with the GDPR);
- Contacts, representatives, signatories, administrators, ultimate stakeholders and employees of our B2B customers, other contact parties and potential customers;
- Visitors to our website.

Types of personal data and sources from which personal data originates

Within the framework of our services, we may collect personal data with regard to:

Contract request: Via our website or via your contact within our organisation, you can contact us directly about DaaS products and/or services. Via this direct contact, you can subsequently pass on specific data to us, e.g. your (business) contact data such as first name, surname, email address, telephone number, the name of the organisation where you work, your job title and possibly other personal data that you are giving us when you communicate with us.

Contract request: If we agree on a DaaS contract with you, we require some data in order to finalise the contract and to subsequently execute it. Examples of this data includes (business) contact details such as first name and surname, email address, telephone number, the name of the organisation where you work and your job title. Other examples include your (business) delivery address, (digital) signature, extracts from the Chamber of Commerce and data about the DaaS contract.

Website visit: During a visit to our website, your browser will transfer the following data types that are subsequently saved on our system: the IP address of the computer, the server requests (for example, requested pages) and the time, the browser type and the referrer URL (this is the address of the website that you visited before visiting ours if you arrived at our website via a hyperlink).

These first three data types are technically required to be able to properly display the webpages you accessed. In addition, we can use this data to securely manage this website (for example, protecting the website against hacking). The referral URL is anonymised and used to compile statistics for marketing purposes. For security reasons and especially to protect our web servers against attacks, this type of data is also saved for a specific period in accordance with Article 6, paragraph 1 (f), of the EU GDPR.

Newsletters: You can subscribe to our newsletter through our website. To send you our newsletter, we need to process your first name and surname, telephone number, email address,

the name of the organisation where you work and your job title. We apply anonymous link tracking for statistical reasons.

Downloading digital information: You can download digital information through our website. To download this information, we will ask for your first name and surname, telephone number, email address, the name of the organisation where you work and your job title.

Public registers: Information is publicly accessible to us through public registers such as, for example, at the Chamber of Commerce or on public websites.

Objectives and legal bases for data processing

The provisions of the EU GDPR and all other applicable provisions regarding data protection are observed when processing personal data. Legal bases for data processing arise in particular from Article 6 of the EU GDPR. The legal bases for our processing activities are:

Executing an agreement: Personal data needs to be processed (i) for realising DaaS products and/or services and to enter into and execute the agreements linked to them including in any case the DaaS contract, (ii) to instruct and communicate with third parties in relation to delivering DaaS products and/or services including the financial company and hauliers, (iii) for CMDB reporting where all primary configuration items are related to the end user to whom the DaaS product is allocated, (iv) for the installation of HP Techpulse monitoring software so that the technical health of the device can be monitored and (v) for objectives in relation to customer administration to register and manage your file(s), your return shipments and the status of returned products and to remove personal data that has remained behind regarding returned products.

Important: The personal data that we ask you to provide is therefore required for (entering into and/or executing) the DaaS contract. If you do not provide the requested data, we may not be able to deliver the required products and/or services.

Legal obligation: The processing of personal data is required (i) for objectives related to the financial administration and customer administration and (ii) to comply with legal obligations in relation the administration and taxation.

Legitimate interest: The processing of personal data is required (i) to give support and to communicate with you about the contract, the services, the products, the product guarantees or other aspects related to DaaS. This will, for example, ensure that you can log a ticket through the Service Now ticket system or ask for assistance via the ARP Support Desk; (ii) for the use for the Oracle Eloqua software system so that we can contact you directly when you download digital information through our website and you leave your data with us; (iii) for the use of the CORE contract management system so that we can draw up quotations for you and/or so that we can efficiently manage accepted quotations and/or entered into contracts; (iv) for marketing objectives to inform you about new or similar products or services and to organise and manage promotional events; (v) to perform investigations and analyses and improve our services, products and the quality thereof; (vi) to process complaints, disputes, procedures and legal actions in relation to our DaaS products and services and to safeguard our legal position in relation to this and (vii) to prevent or trace fraud or abuse and protect our assets, business activities and staff.

Permission: If the applicable legislation prescribes this, we process your personal data after you have given us express permission. If you have given us your permission, you can retract your permission at any time. You can do this by contacting with the CoE directly via mcoe@bechtle.com.

Important: The processing of special categories of personal data as referred to in Article 9, paragraph 1, of the EU GDPR will then only take place if this is required based on legal rules and there is no reason to assume that your legitimate interests prevail when the processing is excluded.

Age

Our website does not focus on people who are younger than 16 and we do not have the intention of collecting data about website visitors who are younger than 16.We cannot, however, check whether a visitor is older than 16.We therefore recommend to parents to be involved in the online activities of their children to prevent data about children being collected without parental consent.If you are convinced that we have collected personal data about a minor without this consent, please contact us via mcoe@bechtle.com. We will then remove this data.

Retention period for data

We save your data for as long as we need the data for the relevant processing objective. Personal data that has been acquired within the context of the DaaS contract is kept during the entire duration of the contract and agreements that are related to this that we have entered into with you and, after termination thereof, in accordance with the legal time limits.

Personal data that is on a returned DaaS device is removed.

Please be aware that many retention periods determine that data must be further stored. This mainly concerns mandatory taxation/legal retention obligations. We will therefore only keep your personal data during longer periods when we must from a legal perspective (for example, due to legal regulations with regard to administration obligations, retention duties or taxation obligations) or when this is required to protect our interests within the framework of legal proceedings.

For more information about the specific retention periods that apply to your personal data, you can contact the CoE via mcoe@bechtle.com.

Issuing data to third parties

In relation to the aforementioned objectives, we may share your personal data with third parties such as service providers that we engage for the execution of the DaaS contract that we have entered into with your company. This may concern financial companies and service providers such as the ARP CoE and ARP Support Desk that we deploy for the delivery of our products and for maintenance and repair services.

Finance companies: We use finance parties for lease solutions. For the allocation of the DaaS contract to the finance party, we issue to them specific required personal data (such as your name, your (business) contact details and information about the DaaS contract). The finance party will, moreover, process your personal data with a view to carry out credit checks within the framework of the DaaS contract. For more information about the way in which the finance party deals with your personal data as an independent processing responsible party, you can consult their privacy policy by using the link below.

- Privacy | HPE

Business consultants: In addition, we may issue your personal data to our business consultants (taxation and legal advisers, lawyers, accountants and auditors), banks, partners, insurers, affiliated companies, legal successors, marketing agencies and entities that offer IT services insofar as this is necessary and only insofar as this is permitted in accordance with the applicable legislation.

Google: We will share your contact details with Google for implementation services and support. For more information about the way in which Google deals with your personal data, you can consult the privacy policy of Google via https://privacy.google.com/businesses/compliance/.

HP Techpulse: We share your personal data with HP Techpulse so that the technical health of the device can be monitored.

Service Now: We share your personal data with Service Now for logging tickets.

CORE: We share your personal data with CORE so that we can draw up quotations for you and can manage accepted quotations and/or entered into contracts.

Oracle Eloqua: We share your personal data with Oracle Eloqua so that we can contact you directly when you download digital information via our website and leave your data behind.

Government agencies: We also share your personal data with the competent government agencies if we have an obligation to do so, for example in the case when the tax authorities ask us to issue specific documents that specifies your personal data.

Authorities: Should we suspect fraud or abuse of our website, we can, of course, transfer personal data to the competent authorities. This will then occur based on the legitimate interest that we and others have that our website is not abused for fraudulent or other unlawful objectives.

Important: We will ensure that contractual safeguards are applied where required to guarantee the protection of your personal data when we pass on your personal data to a third party.

Issuing data abroad

Due to our international nature (ARP Nederland B.V. affiliated to the "Bechtle AG" group), data that you give us may be passed onto companies and trusted third parties affiliated to ARP Nederland B.V. or they may gain access to the data. This means that your personal data may be processed outside the country where you reside if this is required to realise the objectives specified in this privacy policy.

The transfer of data to third countries (countries outside the European Union and the European Economic Area, respectively) only takes place insofar as this is legally prescribed, if you have granted us permission to do so or if this is required to realise the objectives specified in this privacy policy. An attempt is made, in such a case, to safeguard the observance of the data protection level through binding EU Standard Contractual Clauses, business regulations regarding data protection, etc.

Secure data transfer

In order to protect the data that is stored with us as best as possible, we use technical and organisational protection measures that are in accordance with the applicable legislation with regard to data protection. This also means that we demand from our service providers that they take suitable measures to protect the confidentiality and protection of your data. Unfortunately, there is not a single data transfer or storage system that can be guaranteed to be 100 % secure. Depending on the state of the art, the costs of implementation and the nature of the data to be protected, we take technical and organisational measures to prevent risks such as destruction, loss, change and unauthorised publication of or access to your data. If you believe that your interaction with us is no longer secure or your data is no longer being processed by us in a secure manner, please immediately contact the CoE via mcoe@bechtle.com.

You, of course, also have a number of responsibilities to ensure that the data that you issue to us is correct, full and up-to-date to the best of your knowledge. It is, furthermore, your responsibility, when you share data from other people with us, to collect this data in accordance with the local legal requirements. You must, for example, inform such other people regarding whom you issue data to us about the content of this privacy policy and obtain their prior permission.

Automated individual decisions

Our organisation does not use entirely automated processing processes to arrive at a decision.

If a negative decision has been taken about you based on automatic decision-taking and/or profiling and you disagree with this, please contact **the CoE via** mcoe@bechtle.com. We will then remove this data.

Websites of third parties

This policy does not apply to websites of third parties that are linked to this website. We cannot guarantee that these third parties deal with your personal data in a reliable or secure manner. We recommend reading the privacy policy of these websites before using these websites.

Privacy policy changes

We reserve the right to amend this privacy policy. Changes will be published on this website. We recommend regularly consulting this policy so that you are aware of these changes.

Data Protection Authority

We will naturally also be happy to assist you when you wish to make a complaint about the processing of your personal data. Based on privacy legislation, you are entitled to submit a complaint to the Data Protection Authority about our processing of your personal data. Contact the Data Protection Authority for this.

Cookies

Our website uses cookies or comparable technologies where information about your device is saved and/or read out. For more information about which cookies we use, why and how and what your choices are within this context, click here for our cookie policy.

Questions

If you have any questions about the content of this privacy policy, you can contact your contact at our organisation at any time. If your contact is not immediately reachable due to specific circumstances, you can always use the following contact details:

ARP Nederland B.V.
Withuisveld 30
6226 NV Maastricht, the Netherlands
Tel. no.: +31 43 855 0000
Email: mcoe@bechtle.com

Important: Please refer to the contact details of ARP Nederland B.V. since DaaS activities are managed from ARP Nederland B.V.