PRIVACY POLICY

Embrace-IT ApS

Date: 21 May 2018

1 Responsibility

1.1 Protecting your Personal Data is our highest priority regardless of whether such Personal Data relates to you, your transactions, your products or your services.

1.2 We process Personal Data and have therefore adopted this Privacy Policy, which tells you how we process your Personal Data.

2 Service Provider

2.1 Service provider is:

Embrace-IT ApS
VAT No. 36942320
Kildehøjvej 12
Dk-3460 Birkerød
Denmark

T: [+45] 45 3615 3600
E: info@embrace-it.com
www.embrace-it.com

3 Personal Data

3.1 It is important for us to keep your Personal Data safe and confidential. We have procedures for collecting, storing, deleting, updating and disclosing Personal Data to prevent unauthorized access to your Personal Data and to comply with applicable laws.

3.2 We ensure fair and transparent computing. When we ask you to provide us with your Personal Data, we will let you know what Personal Data we process about you and for what purpose such Personal Data is being processed. You will receive information about this at the time of collection of your Personal Data.

3.3 The following guidelines describe the types of Personal Data we collect, how we process such Personal Data, and who you can contact, if you have any questions or comments about this Privacy Policy.

4 Categories of Personal Data

CUSTOMER

4.1 We will collect and process the following Personal Data pertaining to You or the Data Subject, which may include:

- First name and last name
- Email address
- Name of affiliated legal entity or company
- Password-based Key (with random salt, HMAC digest algorithm)
- Assignment of Data Subject to company units, e.g. country/department/team
- Email templates
- Time zone
- IP Address
- OS Name & Version
- Browser Name & Version
- Screen Resolution
- Language (based on headers sent by browser)
- Usage Date & Time

EMPLOYEE:

4.2 We will collect and process the following Personal Data pertaining to You or the Data Subject, which may include:

- General Personal Data (e.g. name and/or username, address, e-mail, date of birth, gender, profile picture, location, etc.)
- Social Security number
- Information about close family
- Information about education
- Opinions
- Former occupation
- Current position
- Tasks
- Working hours and other service conditions
- Information about salary and tax
- Information on sickness absence and illness and other absence from work
- Pension information
- Withholding tax information
- Information about the account number to which salary must be assigned.
- Sensitive data
- Biometric information
- Traffic data on using the Internet
- Localization data from the Internet, mobile, GPS or camera
- Transaction Data
- Unique numbers on network devices

- E-mails
- Social information

5 Purpose

5.1 We collect and store your Personal Data for specific purposes or other legitimate business purposes.

5.2 Your Personal Data is collected and used for:

CUSTOMER

- to provide you with Embrace's service information and news,
- to support Embrace and services offered on or through Embrace,
- to contact you for feedback about our services,
- to conduct research about Embrace's customer base or services,
- to fulfil your reservation and purchase requests,
- to process your payments including credit checks and collection,
- to notify you of technical updates or changes in policy,
- to contact you for our own marketing and promotional purposes, or
- to process contests, sweepstakes, or other promotions and fulfil any related awards or discounts.

EMPLOYEE

- Management and fulfilment of our employment agreement with you or action upon your request
- Managing your relationship with us
- Compliance with legal requirements

- Other

5.3 We may use non-Personal Data such as demographic data to analyse and develop our marketing strategy and further improve embrace-it.com and our services.

6 The Data Subjects' rights

6.1 The Data Subjects' rights will only be individually important in relation to Embrace in the cases where Embrace is data controller. If Embrace is data processor, the Data Subjects' rights must be fulfilled by the data controller who will typically be Embrace's customer.

6.2 Right of access

6.2.1 According to article 15 of the General Data Protection Regulation, the Data Subject is entitled to be informed whether any Personal Data about the subject is being processed and if so, obtain access to the Personal Data (a copy of the Personal Data must be handed over).

6.2.2 Furthermore, the Data Subject is entitled to receive the following information:

- the purpose of the processing
- the affected categories of Personal Data
- the recipients or categories of recipient, the Personal Data has been or will be passed on to, particularly recipients in third countries or international organisations
- if possible the period in which the Personal Data will be stored or, if this is not possible, the criteria used for determining this period
- the right to request the data controller for rectification or erasure of Personal Data or limitation of the processing of Personal Data regarding the Data Subject or to object to such processing
- the right to complain to a supervisory authority
- any available piece of information about the origins of the Personal Data if it has not been collected from the Data Subject

- the occurrence of automated decisions, including profiling as described in article 22(1) and (4) and, as a minimum, meaningful information about the logic hereof as well as the importance and the expected consequences for the Data Subject of such processing.

6.2.3 Furthermore, the Data Subject is entitled to receive information about the necessary guarantees if the Personal Data has been transferred to third countries.

6.2.4 In order to comply with a request for access we shall search all systems - including all databases, all hardware and all portable media - as well as all physical materials which are part of a register and hand over the Personal Data that has been registered about the Data Subject.

6.2.5 According to the General Data Protection Regulation the right to access does not apply if the Data Subject's interest in the information is considered to be of less importance than fundamental concerns for personal interests, including the concern for said subject.

6.3 Data portability

6.3.1 Furthermore, according to article 20 of the General Data Protection Regulation the Data Subject is entitled to receive Personal Data about himself which said subject has provided to the company. This data must be provided in a structured, commonly used and machine readable format.

6.3.2 The Data Subject is also entitled to transmit this information to another data controller himself without objections from the company when the processing is based on consent and carried out automatically. If the Data Subject makes use of this right to data portability, the Data Subject is also entitled to have Personal Data transmitted directly from one data controller to another, if this is technically possible.

6.3.3 The right to data portability only comprises information received from the Data Subject and will only comprise automatic processing. Further, the right to data portability will be very limited if the company bases its right to process Personal Data on any other legal rights to process Personal Dta than consent.

6.4 Right to rectification

6.4.1 According to article 16 of the General Data Protection Regulation, the Data Subject is entitled to obtain rectification of incorrect Personal Data by the data con-

troller without undue delay. Taking the purpose of the processing into consideration, the Data Subject is also entitled to obtain completion of incomplete Personal Data, e.g. by submitting a supplementary statement.

6.4.2 This right supplements our own basic obligation to continually ensure that only correct and updated information is processed, cf. article 5(1), point d.

6.4.3 However, the right to rectification only applies to objective Personal Data and not to subjective assessments. The fact that we may have decided that an employee does not have legal basis to conduct a case is not considered to be Personal Data governed by the right to rectification.

6.5 Right to be forgotten

6.5.1 According to article 17 of the General Data Protection Regulation, the Data Subject is entitled to request erasure of Personal Data by us without undue delay. In that case we are obliged to erase Personal Data without undue delay.

6.5.2 However, this right is limited in such a manner that the Data Subject cannot request erasure if the processing is necessary in order to comply with a legal obligation or to establish, exercise or defend legal claims, cf. article 17(3), points b and e.

6.5.3 We believe that the ”right to be forgotten” will very rarely be relevant for the Personal Data collected by us. It may become relevant if the collection of Personal Data was never necessary and therefore should not have been carried out or if the Personal Data is undoubtedly no longer necessary. In that case the obligation to erase Personal Data will also follow from the basic obligation to only process necessary information, cf. article 5(1), point c of the General Data Protection Regulation. However, the “Right to be forgotten” shall not apply if (and for as long as) we store such Personal Data in order to refute a possible legal claim from customers.

6.5.4 If, according to article 17, we are obliged to erase Personal Data, which has been transferred to other data controllers or data processors, we must inform such data controllers and data processors of the request for erasure of all links to or copies or reproductions of said Personal Data.

6.6 Right to object - also against automated decisions

6.6.1 It follows from article 21 of the General Data Protection Regulation that the Data Subject may at any time exercise his right to object to the processing of his Personal Data, if the processing - including profiling - is based on article 6(1), point e or f. These provisions govern the right to process ordinary Personal Data if the processing is necessary to carry out a task in the interest of society or if the processing is necessary to pursue a legitimate interest and the concern for the Data Subject does not exceed this interest.

6.6.2 If an objection is filed we are no longer entitled to process said Personal Data unless we can prove substantial legitimate reasons for the processing which supersedes the interests of the Data Subject or if the processing is necessary in order to establish, exercise or defend legal claims.

6.6.3 We believe that this provision will only have limited impact on our processing because our processing of Personal Data is to a wide extent tied to the authority to comply with an agreement or establish a legal claim just as we - if the processing otherwise complies with the basic processing rules - will often be able to show substantial legitimate reasons for processing the Personal Data.

6.6.4 The provision in article 21 is based on the condition that the Data Subject is made specifically aware of his right to object and that this information must be given no later than at the time of the first communication. Furthermore, this information must be given in clear terms and kept separate from other information.

6.6.5 In addition to article 21, article 22 provides the Data Subject with a right to not be subject to a decision which is solely based on automated processing, including profiling, which has legal effect or similar considerable effect on said person.

6.6.6 This provision also includes several exceptions, cf. article 22(2). Among other things, this right does not apply if the decision is necessary to enter into or comply with an agreement between the Data Subject and data controller, if the processing is in accordance with the law or if the processing is based on the Data Subject's explicit consent.

6.6.7 However, article 22 generally presumes that automated decisions are not based on specific categories of Personal Data, cf. article 9(1), unless explicit consent has been given and sufficient measures have been taken to protect the Data Subject's rights and civic rights and legitimate interests.

6.7 <u>Right to restriction of processing</u>

6.7.1 Article 18 of the General Data Protection Regulation gives the Data Subject the right to obtain from the data controller restriction of processing where one of the following applies:

- the accuracy of the Personal Data is contested by the Data Subject, for a period enabling the controller to verify the accuracy of the Personal Data
- the processing is unlawful and the Data Subject opposes the erasure of the Personal Data and requests the restriction of their use instead
- the controller no longer needs the Personal Data for the purposes of the processing, but back up of the Persona Data are required for the establishment, exercise or defence of legal claims
- the Data Subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the Data Subject.

6.7.2 Thus, this right is an alternative (and smaller) interference in the processing compared to the Data Subject's right to object under articles 21 and 22 and the Data Subject's "right to be forgotten" under article 17.

6.7.3 It follows from subsection 2 of this provision that if processing has been restricted, such Personal Data may, except for purposes of storage, still be processed if, among other things, the Data Subject consents or if the processing is necessary to establish, exercise or defend a legal claim.

6.7.4 In our opinion this provision will only have limited importance for our access to process Personal Data as part of our case work.

7 General processing principles

7.1 Processing principles

7.1.1 We will process Personal Data in a legal, reasonable and transparent.

7.1.2 Our processing of Personal Data is subject to purpose limitation which means that Personal Data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes,

7.1.3 We carry out restrictive processing of Personal Data which means that it must be sufficient, relevant and limited to the necessary data for the purposes for which it is processed.

7.1.4 Personal Data must be processed in accordance with a principle of accuracy which means that it must be correct and, if necessary, updated.

7.1.5 We process Personal Data in accordance with a principle of storage limitation which means that Personal Data must be stored in such a way that the Data Subjects cannot be identified for any longer than what is necessary for the purposes for which the relevant Personal Data is processed.

7.1.6 Personal Data must be processed in accordance with principles of integrity and confidentiality which means that it must be processed in such a way that the Personal Data is kept sufficiently safe and protected against unauthorised or unlawful processing and accidental loss, destruction or damage, by using adequate technical or organisational measures.

7.2 Risk analysis

7.2.1 In connection with our case work we must carry out adequate technical and organisational measures in order to ensure a level of security which corresponds to the risks that are specifically related to our processing of Personal Data.

7.2.2 We have carried out a risk analysis which forms the basis of this Privacy Policy.

7.3 Data Protection Impact Assessment (DPIA)

7.3.1 Article 35 of the General Data Protection Regulation contains a requirement that where a type of processing, in particular when using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the data controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of Personal Data.

7.3.2 The duty to carry out an assessment of the impact only applies to specific cases where a high risk to the rights and freedoms of natural persons is found.

7.3.3 A data protection impact assessment shall be required in the case of:

a) processing on a large scale of special categories of data or of Personal Data relating to criminal convictions and offences, or

b) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person, or

c) a systematic monitoring of a publicly accessible area on a large scale.

7.3.4 It is our assessment that we will rarely carry out processing which complies with one of the above criteria. Therefore, we expect that the provisions governing impact assessment will have relatively little impact on our processing of Personal Data about customers.

7.3.5 If an impact assessment is carried out anyway, the result of the assessment will be taken into consideration when adequate measures need to be taken.

7.4 Data Protection Officer (DPO)

7.4.1 The duty to appoint a Data Protection Officer is, according to article 37 of the General Data Protection Regulation, conditioned upon the fact that processing of Personal Data is ”core activity”. This is neither the case where Embrace acts as data processor, nor in situations where Embrace acts as data controller.

7.4.2 The data controller and the data processor shall designate a Data Protection Officer in any case where:

a) the core activities consist of processing operations which, by their nature, their scope and/or their purposes, require regular and systematic monitoring of Data Subjects on a large scale, or

b) the core activities consist of processing on a large scale of special categories of data, or

c) the core activities consist of processing on a large scale of Personal Data relating to criminal convictions and offences.

7.4.3 It is our assessment that Embrace does not process Personal Data on a scale as described above. We have therefore chosen not to appoint a Data Protection Officer.

7.4.4 Because of the principle of accountability we have - irrespective of whether we are acting as data controller or data processor - appointed a person within our organisation that is responsible for carrying out the assessments and the advice service which is usually carried out by a Data Protection Officer.

7.5 Data controller

7.5.1 With regard to Personal Data about employees and information about Embrace's customers, Embrace will predominantly work as data controller. Embrace will independently assess whether there is basis for collecting/processing Personal Data which is relevant and necessary and for how long the Personal Data should be stored. In these cases where Embrace primarly provides it suppoer and services, Enbrace will act as data processor.

7.6 Data processing agreement

7.6.1 In cases where we are data controllers and have assessed that the arrangement with the data processor constitutes a data processing structure, we will prepare a data processing agreement.

7.6.2 The data processing agreement must be entered into between us (the data controller) and the other party (the data processor) and must comply with the requirements to data processing agreements as set out in the General Data Protection Regulation, cf. article 28(3) of the General Data Protection Regulation. This means that a contract or another legal document which is binding for the data processor must be prepared. Furthermore, it is a requirement that the data processing agreement is in writing, including electronic form.

7.6.3 Furthermore, the General Data Protection Regulation sets out several specific requirements to the contents of the data processing agreement. The contract must, among other things, set out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of Personal Data and categories of Data Subjects and the obligations and rights of the controller as well as the obligations of the data processor with respect to carrying out the task. These requirements are described in detail in article 28(3), points a-h of the General Data Protection Regulation.

7.6.4 If we act as data processor for the customer, we must enter a written data processing agreement with the customer.

7.7 Transfer to third countries

7.7.1 There will be no transfer of Personal Data to third countries.

7.8 Data processors - an overview

7.8.1 The technical operation of Embrace is carried out by external companies. These companies act as data processors of the Personal Data for which we are data controllers.

7.8.2 The data processing is carried out within the European Union.

7.8.3 The data processor acts solely under our instruction.

7.8.4 We use the following data processors:

Data processor	**Location**	**Contract type**
	Denmark	Data processing agreement

7.8.5 The data processor has taken the necessary technical and organisational security measures to ensure that the Personal Data is not accidentally or illegally destroyed, lost or impaired and that it does not become known to unauthorised persons, is abused or in any other way processed in a manner that violates the Data Protection Act. The data processor will upon request - and against payment of the data processors at any time applicable hourly rates for such work - provide you with sufficient Personal Data to prove that the data processor has taken the necessary technical and organisational security measures.

7.9 Transfer – customer data

7.9.1 We may disclose Personal Data to other companies or people under any of the following circumstances:

- if sharing the information is reasonably necessary to provide or otherwise make available Embrace and any feature of Embrace or a service that you have requested.

- to keep you up to date on the latest product announcements, software updates, special offers, or other information we think you would like to hear about either from us or from our business partners (unless you have opted out of these

types of communications). (Note that you will not be able to opt out of service announcements that contain important information relevant to your use of Embrace and are not promotional in nature.)

- if we believe in good faith that we are required to do so by law, about litigation, to prevent a crime, or to protect personal property, the public, or Embrace.

- about a sale or merger with another entity, consolidation, restructuring, sale of company assets, financing or other corporate change, including during the course of any due diligence process or if Embrace should ever file for bankruptcy or related proceeding.

- when we otherwise have the Data Subject's consent to share the information.

- Embrace may also share non-Personal Data with third parties (e.g. aggregate or demographic data).

7.10 Transfer – employee data

7.10.1 We may disclose Personal Data to other companies or people under any of the following circumstances:

- if sharing the information is reasonably necessary for administration of the employee relationship we have with you, e.g. for purposes of calculation of salaries, employee benefits, tax calculation, etc.

- if we believe in good faith that we are required to do so by law, in connection with litigation, to prevent a crime, or to protect personal property, the public, or Embrace.

- in connection with a sale or merger with another entity, consolidation, restructuring, sale of company assets, financing or other corporate change, including during the course of any due diligence process or if Embrace should ever file for bankruptcy or related proceeding.

- when we otherwise have the Data Subject's consent to share the information

7.11 Transfer to social media networks

7.11.1 No Personal Data will be transferred to any social media network.

7.12 Other transfers

7.12.1 If we receive a request from the police (or similar public authority) or the court system to hand over Personal Data, we will hand over your Personal Data in accordance with applicable law.

7.13 Disclosure for legal reasons

7.13.1 We disclose Personal Data to companies, organizations or individuals outside of our group of companies if we believe in good faith that access, use, preservation or disclosure is necessary to: (1) comply with applicable law, regulation, legal process or enforceable governmental request, (2) enforce applicable user terms, including investigation of potential violations, (3) register, prevent or otherwise protect against address fraud, security or technical issues, or (4) indemnifying us, our users or the public's rights, property or safety, as required.

7.14 Other disclosure

7.14.1 Embrace does not use your Personal Data for profiling.

7.15 General technical measures

7.15.1 The Danish Data Protection Agency's IT security guidelines, cf. below, form the basis of the considerations and assessments we have carried out under the General Data Protection Regulation.

7.15.2 Access to Personal Data is restricted to persons who have a material need for access to Personal Data. Personal Data will only be accessed on a "need to know" basis.

7.15.3 Employees, who handle Personal Data, are instructed and trained in what they must do with Personal Data and how to protect Personal Data.

7.15.4 There must be as few people as possible with access to Personal Data, with due regard for the operation. However, there must be a sufficient number of employees to ensure the operation of the tasks concerned in case of sickness, holidays, staff replacement, etc. Personal Data will only be accessed on a "need to know" basis.

7.15.5 Personal Data on paper - for example in cartons and binders- are kept closed and locked when not in use.

7.15.6 When documents (papers, charts, etc.) are discarded, shredding and other measures are used to prevent unauthorized access to Personal Data.

7.15.7 We use access codes to access PCs and other electronic equipment with Personal Data. Only those who need to have access will receive an access code and then only for the systems that they need to use. Those who have a password may not leave the code to others or leave it so others can see it. Checking of assigned codes must be done at least once every six months.

7.15.8 Unsuccessful attempts to access IT systems with Personal Data are detected and logged. If a specified number of consecutive rejected access attempts is detected, further tests must be blocked.

7.15.9 We have appointed a responsible person to monitor such inaccessible access attempts. Taking into account the technological development, software is available that can clarify who has attempted to gain access to Personal Data.

7.15.10 If Personal Data is stored on a USB key, Personal Data must be protected, e.g. by use of a password and encryption key. Otherwise, the USB key must be stored in a locked drawer or cabinet. Similar requirements apply to the storage of Personal Data on other portable data media.

7.15.11 PCs connected to the Internet shall have an updated firewall and virus control installed. When connecting to WiFi, for free access, we ensure appropriate security measures taking into account the current state of technology development in the IT-area.

7.15.12 If sensitive Personal Data or social security numbers are sent by e-mail via the Internet, such e-mails must be encrypted. If you send Personal Data to us via email, please note that sending to us is not secure if your emails are not encrypted.

7.15.13 In connection with the repair and service of data equipment containing Personal Data and when data media are to be sold or discarded, we take the necessary measures to prevent information from being disclosed to a third party.

7.15.14 In the situations where a computer is submitted for repair and where Personal Data is stored on such computer, we establish several access codes for different sections of the Personal Data. For example, a repairer will not need to be able to access Personal Data that may be on the computer. Such a multi-code scheme may help - but not eliminate - the risk of misuse of Personal Data. In addition, agree-

ment and verification should ensure that repairers do not unduly access Personal Data, for example, by using confidentiality statements.

7.15.15 When we use an external data processing agent to handle Personal Data, a written data processing agreement is signed between us and the data processor. This applies, for example, when we use an external document archive or if cloud systems are used in the processing of Personal Data - including communication with the customer. In the same way, a written agreement between us and our customer is always entered into if we act as data processor. Data processing agreements are also available electronically.

7.15.16 We have internal rules on information security. We have adopted internal rules on information security that contain instructions and measures which protect Personal Data from being destroyed, lost or modified, from unauthorized disclosure, and against unauthorized access or knowledge of them. We will ensure that collected Personal Data are treated with care and protected according to applicable safety standards. We have strict security procedures for collecting, storing and transferring Personal Data to prevent unauthorized access and compliance with applicable laws.

7.15.17 We have taken the necessary technical and organizational safeguards to protect your Personal Data from accidental or illegal destruction, loss or change, and against unauthorized disclosure, abuse or other actions contrary to applicable law.

7.15.18 The systems are located on servers in secured premises.

7.15.19 We use industry standards such as firewalls and authentication protection to protect your Personal Data.

7.15.20 All data transferred between client (browser and web app) and server(s) are encrypted according to the HTTPS protocol.

7.15.21 All production facilities are locked and only staff members who have signed a declaration of confidentiality have access to the production facilities. After the end of normal working hours, the production facilities are locked. Access to the production facilities is always carried out under the supervision of an employee.

7.15.22 All access to our premises is logged by electronic key or entered in the guestbook.

7.15.23 We take a backup of all databases and files on shared drives every night. The backup is stored on an internal server, partly on an external data centre.

7.16 Back-up

7.16.1 We make the following types of backup:
a) Rolling backup. This method takes daily backup of all file and data updates and creates a backup of all new data. This creates a history of changes so that the ability to recover lost data is increased.
b) backup clone. This backup strategy creates a perfect copy of each device on the network
c) backup offsite. This backup ensures against data loss if backup is stored on site. All data and files are backed up and backup stored offsite.

7.16.2 All backup data and files are overwritten at 30-day intervals. It is not technically possible to complete erasure of individual files on a backup before such overwriting occurs. Thus, if you have requested that we erase Personal Data, such Personal Data will be erased in live environment, but will remain on backup until the specific backup is overwritten after 30 days. However, we have introduced internal processes and procedures to ensure that Personal Data is not reintroduced as live data by reloading data and files from a backup as Personal Data has been erased according to the "right to be forgotten."

7.17 Erasure - when

7.17.1 When an assignment from a customer has ended, we will have no further need to process the Personal Data. The assignment has been solved.

7.17.2 However, several other considerations and special provisions mean that Personal Data should not or cannot be erased until some time has passed.

7.17.3 The period in which the Personal Data is stored before erasure should be decided.

7.17.4 Under the book keeping rules, Personal Data related to a payment must be kept for 5 years + the current calendar year after the end of the accounting year.

7.17.5 To ensure that we are able to represent our interests in case of a liability suit Personal Data can be stored for 3 years after the end of the assignment.

7.17.6 To ensure the logical synergi with the processing of accounts, customer data should be stored for 5 years after the termination of the customer relationship.

7.17.7 Contact information - CRM must be continuously erased and updated. Emails which may be important for the determination of a legal claim must be stored for 5 years and then erased, unless legal claims have been submitted against or may be submitted by Embrace.

7.18 Erasure - how

7.18.1 It appears from IT security text ST3 from the Danish Data Protection Agency regarding the erasure of Personal Data that erasure of Personal Data means that Personal Data is irrevocably removed from all storage media on which they have been stored and that Personal Data cannot be recreated in any form. In that connection, it is necessary to pay attention to all storage media - including portable storage media such as laptops, USB sticks etc. as well as back up.

7.18.2 To facilitate the erasure process, all physical material must be scanned to the electronic case and then shredded or returned to the customer.

7.18.3 Alternatively, Personal Data may be completely anonymised with the result that they cannot be ascribed to a specific person. In this case, the General Data Protection Regulation does not apply and complete anonymisation is therefore an alternative to deletion. It is, however, important to remember that anonymization as an alternative to deletion is conditioned upon deletion of all traces that may lead to the person, the data concerns. This is often a very difficult task.

7.18.4 Following deletion/anonymisation we will carry out appropriate cross checks in the form of searches for name/CPR-no. etc. regarding the customer and the case to ensure that nothing appears.

7.18.5 Duty to disclose - Customer

7.19 Each customer receives a link to our Privacy Policy.

8 Detailed processing rules - Customer

8.1 Authority to process

8.1.1 Our authority to process Personal Data is primarily based on the relationship to our customer and our ability to administrate agreements we have entered into. In general, we will have the authority to process the necessary data within the framework of this assignment. This specifically follows from the General Data

Protection Regulation, article 6(1), points a-c and point f as well as article 9(2), points a and f.

8.1.2 These provisions govern the right to process Personal Data, (i) if there is consent, (ii) if the processing is necessary to fulfil the terms of an agreement, (iii) if the processing is necessary in order to comply with a legal requirement, (iv) necessary in order to comply with significant interests that supersede the interests of the Data Subject; or (v) necessary in order to ensure that a legal claim may be established, exercised or defended.

8.1.3 We are authorised to process civil registration numbers (i) when it follows from the law, (ii) if there is consent; or (iii) if it is necessary to establish a legal claim, cf. the Danish Data Protection Act, section 11, cf. section 7.

8.1.4 We believe our processing of Personal Data with respect to a customer to a wide extent will have its authorisation in the above-mentioned provisions.

8.2 Activation

8.2.1 We collect Personal Data from you and the Data Subject when you activate the service we provide and when you and the Data Subject use embrace-it.com.

8.3 Visit on our Website

8.3.1 When you visit embrace-it.com, we also collect non-Personal Data, which is information that by itself cannot be used to identify or contact you, such as demographic information (e.g. age or gender) or usage information (e.g. the browser you are using, the URL that referred you to Embrace and the areas of Embrace you visit). We may also supplement the information we collect with information from other sources to assist us in evaluating and improving our Platform and offerings.

8.4 IP addresses and browser settings

8.4.1 For each visit to embrace-it.com, the used IP address and browser settings are registered. Your IP address is the address of the computer you use to visit embrace-it.com. Browser settings are, for example, the browser type you are using, browser language, time zone, etc. The IP address and browser settings are registered to ensure that Embrace can always identify the computer used in case of abuse or unauthorized use about the visit to or use of embrace-it.com. The IP ad-

dress is also used to determine your approximate location (at city IP-address level).

8.5 Newsletter

8.5.1 If you subscribe to Embrace's newsletters, your Personal Data will be registered directly with Embrace. If you no longer wish to receive newsletters from Embrace, you can unsubscribe by contacting Embrace on info@embrace-it.com.

8.6 Anonymization

8.7 Embrace applies anonymization of data from customers for statistic and research purposes, as well as to improve systems, processors and products.

8.8 Embrace irrevocably anonymizes Personal Data in such a way that the Data Subject can no longer be identified. For example, name, address or personal identification number will be replaced by a code, serial number, etc. Codes are assigned randomly and cannot be restored using lists, keys, etc., showing the relationship between the serial number and the actual identification information. This also means that Personal Data, such as image, a person's voice, fingerprints or genetic characteristics are erased in aboutonymization.

8.9 Contact Information

8.9.1 Contact information will be updated and permanently erased on a continuous basis. E-mails that may affect the determination of a legal claim must be stored for 5 years and then erased, unless a legal claim has been raised or Embrace suspects one will be raised.

9 Detailed processing rules - Employees

9.1 Authority to process

9.1.1 Our authority to process employee data is based on the following:

- The employee has consented to the use of his Personal Data for one or more specific purposes.
- Processing is necessitated by the compliance with a contract in which the employee is part or by a consideration to the completion of measures that are carried out at the employee's request prior to entering into a contract.

- Processing is necessitated by the compliance with a legal obligation by which we are bound.

- Processing is necessary in order to protect the vital interests of the employees or another natural person.

- Processing is necessary in order to carry out an assignment that is of public interest or which falls under a public authority which we have been instructed to exercise.

- Processing is necessary in order for us or a third party to pursue a legitimate interest, unless the interests or basic rights and civil rights of the employee, which require protection of Personal Data, take precedence.

9.2 Processing of Personal Data prior to the employment

9.2.1 Prior to hiring an employee, we will be processing some standard Personal Data about the employee.

9.2.2 We receive certain Personal Data directly from the applicant, e.g. an application, a CV, photos, diplomas, statements from previous employers and references.

9.2.3 In addition to this, we will collect Personal Data about the applicant. This may consist of publicly available Personal Data on LinkedIn, Facebook or Personal Data which is collected via a standard internet search.

9.2.4 The basis for processing such standard Personal Data, which is processed for selecting an employee for our company, is the General Data Protection Regulation article 6(1), point a, which describes arrangements carried out prior to entering into a contract and the provisions governing balancing of interests, cf. article 6(1), point f.

9.2.5 Photos that are attached to an application may be processed as part of the employment process if the applicant has consented. If photos are used for purposes that go beyong the employment process, the applicant must also consent to this use.

9.2.6 Prior to hiring an employee, we will also in some cases need to process sensitive Personal Data about an employee.

9.2.7 We will ask for your consent to collect Personal Data about you from your current or previous employers by collection of references. You will specifically be asked to sign a declaration of consent of which you will receive a copy. If you do not consent, we will not collect any references.

9.2.8 We will usually ask the employee to provide an extract from the police records (private extract from the police records), but we can also obtain it with the employee's consent (private extract from the police records with consent). Both situations require your consent before we can process the Personal Data. It will usually also be relevant to obtain an extract from the police records about the employment of book keepers and other trusted employees.

9.2.9 We will not collect any credit information about applications unless the employment concerns a highly-trusted position. In this case, we must consider what tasks said employee is authorised to carry out and to what extent the employee is subject to routine controls from e.g. superiors. We will collect credit information about people who apply for the position of book keeper or positions with a more executive financial responsibility. The basis for this processing will be the provisions governing balancing of interests, cf. article 6(1), point f.

9.2.10 In some situations, we will make use of personality tests in connection with hiring new employees. This particularly applies to highly trusted positions. Obviously, such a test can only be carried out with your consent. Irrespective of the fact that the result of a personality test may be considered Personal Data of a more private nature we will generally consider it to be standard Personal Data. However, a personality test may also include sensitive Personal Data. In that case, we require your explicit consent to our processing of Personal Data.

9.2.11 Under certain circumstances we may request Personal Data from you about your health. This may be relevant in cases where an illness will have significant importance for your ability to manage the position. If it is specifically considered to be necessary to obtain information about health, we will state the illnesses or symptoms of illnesses for which we request Personal Data. In this case, the information will be collected with consent.

9.2.12 If you become an employee of our company, the Personal Data we have received and processed during the recruitment process, will be stored on your personnel file throughout your employment and for a subsequent period of 5 years.

9.2.13 If your application is rejected, we will erase the Personal Data we have received and processed during the recruitment process as soon as possible and generally no

later than 6 months after you have received the rejection letter. However, we will at the same time request your consent to store your Personal Data collected during the employment process for a period of 3 years for use in similar employment processes for positions corresponding to the position for which you applied. If we find that an applicant whose application has been rejected will submit a claim under the Equal Treatment Act or the Discrimination Act, Personal Data will be stored for a longer period.

9.3 Processing of Personal Data about current employees

9.3.1 When an employment relationship has been established, we will process additional standard Personal Data. This covers both data that you provide, e.g. your CPR-no., address information, account number etc., information from the employment contract about the job tasks, working hours, salary etc., Personal Data about sickness absence and sickness periods. In addition to this, we will carry out an independent collection of Personal Data about you. This may comprise Personal Data which is registered on an on-going basis from managers and other employee (including minutes of performance reviews) and business partners. Any approach or complaint from other employees or customers/business partners, the management's own collection of Personal Data on social media and inquiries from public authorities concerning the employee etc. will also be included.

9.3.2 If Personal Data is passed on to public authorities, e.g. to the tax authorities concerning income tax etc., the processing is necessitated by the duty to deduct and the duty to report to which we are subject as employers, cf. the applicable tax legislation.

9.3.3 We will only publish work-related Personal Data about employees on our website without prior consent. Publication of Personal Data of a more personal nature, e.g. a photo of the employee, will only be published with the employee's consent.

9.3.4 When an employment relationship has been established, we will under certain circumstances also have to process sensitive Personal Data about you. This may include health information about you, including Personal Data about alcohol abuse and treatment of such abuse, Personal Data about union membership or Personal Data about criminal matters. Private matters and the result of personality tests do not necessarily contain sensitive Personal Data.

9.3.5 In general, it is against the law to process sensitive Personal Data. However, we may under certain circumstances process sensitive Personal Data about an employee. This may particularly be the case if we have received explicit consent

from the employee to process the Personal Data. We will process health information to the extent that it is necessary in accordance with section 56 of the Act on Benefits in the event of Illness or Childbirth without obtaining consent. In such cases, we will process sensitivte health information about chronic illnesses etc. In case of termination where a former employee's right to receive information about the reason for the termination necessitates the registration of such Personal Data, Personal Data may be considered sensitive, if it is accurate and reflects specific actual issues of a social or personal nature about the employee. If Personal Data is only kept in vague and discretionary terms, it is not necessarily considered sensitive.

9.3.6 Personal Data about union memberships may also be processed if the processing is necessitated by our adherence to our obligations under employment law or specific rights which comprise all types of obligations and rights based on employment law.

9.3.7 Other than this, we will only to a limited extent register sensitive Personal Data in a personnel register. The processing must be necessary in order to establish a legal claim, e.g. if we need to register Personal Data about a criminal offense such as embezzlement carried out by the employee if this necessary in order for us to be able to file a claim for damages against the employee.

9.3.8 It may also be necessary to register sensitive Personal Data in cases where there may be a legal claim, e.g. an employee's claim for damages because of a work-related injury.

9.4 <u>Processing of Personal Data about former employees, including erasure</u>

9.4.1 We must erase Personal Data without undue delay. This may be relevant in cases where Personal Data is no longer necessary to fulfil the purpose for which it was collected or otherwise processed.

9.4.2 Personal Data about terminated employees may be stored for up to 5 years after the expiry of the employment relationship. We will, however, store Personal Data for a longer period if the Personal Data is needed to establish, exercise or defend a legal claim, e.g. an employment law case. In such cases, Personal Data may be stored for if it is necessary to conduct the case. A similar allowance may apply about work-related injuries.

9.4.3 In connection with the termination of an employee there may be doubts about when we may transfer the Personal Data in our possession. Any transfer of refer-

ences for an employee which takes place upon request from another company with whom the employee has applied for a job may take place without the employee's consent if the references are considered standard Personal Data. Sensitive Personal Data may only be transferred with the employee's consent.

9.5 Information to the individual

9.5.1 At the time of collecting the Personal Data, we must provide the employee with mandatory information. Furthermore, we must provide supplementary information which is necessary in order to ensure a reasonable and transparent process. If we plan to further process the Personal Data for another purpose than the one for which the Personal Data was collected, we must provide the employee with Personal Data about the other purpose and other relevant additional Personal Data such as time frame, insight, erasure etc. This duty to inform does not apply if the employee is already familiar with Personal Data.

9.5.2 In the other case, where we are collecting Personal Data about an employee from sources other than the employee, must provide the employee with mandatory information hereon. In addition to this, the employee must receive supplementary information which is necessary to ensure a reasonable and transparent processing of the employees Personal Data. The mandatory and supplementary information must be provided to the employee within a specified deadline.

9.5.3 If we aim to further process the Personal Data for another purpose than the one for which it was collected, we must provide the employee with inforation about the other purpose and other relevant additional Personal Data about e.g. deadline, insight, erasure etc. prior to this further processing. The duty to inform does not apply for several cases, including if the employee is already familiar with such information.

9.5.4 Job applicants will be informed if we carry out a credit information agency check and about possible storage of the credit information, including information stating in what cases Personal Data is stored.

9.6 E-mail

9.6.1 Embrace allows for private use of e-mail and the internet available at the workplace. Employees must limit the private use hereof to a reasonable level. Short messages and responses on e-mails are perceived as a reasonable level.

9.6.2 Embrace considers all results and outcome from the use of the company's IT equipment as Embrace's property unless such results or outcome are clearly marked with the term "private". This also applies to your documents and emails. This means that personal e- mails sent / received via your work e-mail may in principle be read by others.

9.6.3 Embrace may review such Personal Data for Embrace to be able to pursue its legitimate interests – such as operation, safety, restoration and documentation as Embrace's need for such use exceeds the employees' need for privacy.

9.6.4 In case of your absence, for example due to illness, vacation or after you have left Embrace, Embrace may assign others access to your folders and your inbox.

9.6.5 Embrace will not read your private e-mails. If a review of your e-mails shows that your inbox contains private e-mails without relation to Embrace, such e-mails will not be read by anyone other than the beneficial recipient. We do not want to read e-mails marked with "private" unless it is clearly stated by the circumstances that a specific e-mail - despite the labelling - is not of a private character or has content that could be a breach of your obligations towards Embrace.

9.6.6 Upon your resignation - voluntarily or involuntarily - your e-mail account at Embrace will only be kept active for a period which is as short as possible from the time where you no longer have access to your personal e-mail account with Embrace. The length of such period will be determined depending on your position and function and may not exceed 12 months. You will not be notified of the final closure of your e-mail account. As soon as you can no longer access your e-mail account, we will put an autoreply on your e-mail account with notice of your resignation and any other relevant information. The active e-mail account will only be used to receive e-mails. We may use the e-mail account to forward any private e-mails to your private e-mail account. Information about your e-mail account will be removed as soon as possible from our website and other publicly available information sites. Only very few trusted employees will then have access to your e-mail account until it is closed.

9.6.7 E-mails shall be erased continuously. E-mails which may affect the determination of a legal claim must be stored for 5 years and then erased, unless legal claims have been raised by or contemplated raised against Embrace.

9.7 Internet

9.7.1 Embrace allows for a reasonable level of private use of e-mails and the internet available at the workplace.

9.7.2 Embrace does not perform systematic, general control of each individual employee's use of the IT-systems. Employee traffic on the Internet and all e-mails sent to and from each employee are registered in a central log file. If abuse is suspected, such as sending private e-mails to a greater extent, or surfing the Internet to a greater extent, Embrace reserves the right to monitor and review employee activities and stored data on Embrace's IT-systems.

9.7.3 Registration for specific internet, such as subscription services or portals, etc. using Embrace's IT-systems, may only take place upon prior written permission from a manager.

9.7.4 Embrace uses firewall / logs, which is a system-technical tool used by the system administrator for security purposes. The integrated logging facilities are necessary for the operation and maintenance of the IT-systems and for security monitoring (system log). A system log may contain Personal Data.

9.7.5 Logging of employees' use of the Internet, which takes the form of a system log on a firewall or other active network components, is to be considered a system log. The system log used is used solely for security purposes.

9.7.6 Embrace may review your use of the Internet for technical and security reasons.

9.8 Home Workplaces

9.8.1 We have ensured that ad hoc jobs, e.g. home workplaces, for employees working from home comply with our IT security rules.

9.8.2 Home workplaces shall meet the following requirements:

- Use of encrypted connections between the ad hoc workplace and Embrace's network,
- Use of two-factor communication,
- Embrace has issued an internal instruction to its employees regarding home workplaces.

9.9 Other Personal Data

9.9.1 Embrace does not collect other types of Personal Data about you.

10 Overview of processing

10.1 Overview of processing for information about customers/suppliers:

Data controller	**Company name, Registration number and contact information** (address, website, telephone and email)	
	The joint data controller and his contact information (address, website, telephone and email)	
	The data controller's representative and his contact information (address, website, telephone and email)	
Purpose(s)	**The purpose(s) of the processing** (a collective, logical coherent purpose of a processing or a number of processing actions which are hereby indicated as one purpose out of the entire list of purposes with the data controller)	
Data Subject categories and Personal Data categories	**Data Subject categories** (e.g. applicants, current or previous employees)	Information is processed about the following Data Subject categories:

	Information which is processed about the Data Subjects (tick off and describe the type of information comprised by the processing activities)	Information which is part of the specific processing. Describe:
Recipients of Personal Data	**Recipient categories to whom information has been or will be transferred, including recipients in third countries and international organisations** (e.g. other authorities, companies, citizens/ customers etc.)	1. Public authorities (if possible specified by name, e.g. tax authorities) 2. Banks 3. Credit agencies
Third countries and international organisations	**Information about transfer of Personal Data to third countries or international organisations** (e.g. data processors' location in third countries, data processor's use of cloud solutions located in third countries)	No (Information about company/partner if it is located in a third country)
Erasure	**Erasure of information** (the expected deadlines for erasure of the various categories of information)	Information about previous employees is erased no later than X years following the end of the journal period in which the personnel case was closed.

		Information about employees is erased no later than X months following the end of the journal period in which the case was closed. Information is continuously transferred to the Danish National Archives in accordance with the provisions of the Archives Act and the rules governing the State Archives.
Technical and organisational security measures	**Description of technical and organisational security measures** (if possible, provide a general description of the technical and organisational security measures, cf. article 32(1))	Processing of Personal Data in connection with HR takes place in accordance with internal guidelines which e.g. set out the scope of the authorisation and access control as well as the logging. Personal Data is both pseudonymised and encrypted before storage and transmitted in an encrypted format. Physical materials are locked away for storage. The following security standards are being used: ISOXXXXX.

10.2 Overview of processing for employee information:

Data controller	**Company name, Registration number and contact information** (address, website, telephone and email)	
	The joint data controller and his contact information (address, website, telephone and email)	
	The data controller's representative and his contact information (address, website, telephone and email)	
Purpose(s)	**The purpose(s) of the processing** (a collective, logical coherent purpose of a processing or a number of processing actions which are hereby indicated as one purpose out of the entire list of purposes with the data controller)	Personnel administration
Data Subject categories and Personal Data categories	**Data Subject categories** (e.g. applicants, current or previous employees)	Information is processed about the following Data Subject categories: a) Applicants b) Employees c) Previous employees
	Information which is processed about the Data Subjects (tick off and describe the	Information which is part of the specific processing. Describe:

	type of information comprised by the processing activities)	Identification information
		Information regarding the employment for use in administration, including position and place of work, salary, information that is relevant to withholding of wages, personnel files, education and sick leave.
		Race or ethnic origin
		Political, religious or philosophical persuasion
		Union membership
		Health information, including genetic data
		Biometric data for the purposes of identification
		Sexual relations
		Criminal offences
Recipients of Personal Data	**Recipient categories to whom information has been or will be transferred, including recipients in third countries and international organisations** (e.g. other authorities, companies, citizens/ customers etc.)	1. Public authorities (if possible specified by name, e.g. tax authorities) 2. Banks 3. Credit agencies

Third countries and international organisations	**Information about transfer of Personal Data to third countries or international organisations** (e.g. data processors' location in third countries, data processor's use of cloud solutions located in third countries)	No (Information about company/partner if it is located in a third country)
Erasure	**Erasure of information** (the expected deadlines for erasure of the various categories of information)	Information about previous employees is erased no later than X years following the end of the journal period in which the personnel case was closed. Information about employees is erased no later than X months following the end of the journal period in which the case was closed. Information is continuously transferred to the Danish National Archives in accordance with the provisions of the Archives Act and the rules governing the State Archives.
Technical and organisational security measures	**Description of technical and organisational security measures** (if possible, provide a general description of the technical and organisational security measures, cf. article 32(1))	Processing of Personal Data in connection with HR takes place in accordance with internal guidelines which e.g. set out the scope of the authorisation and access control as well as the logging.

		Personal Data is both pseudonymised and encrypted before storage and transmitted in an encrypted format. Physical materials are locked away for storage. The following security standards are being used: ISOXXXXX.

11 Questions

If you have questions about this privacy policy or our treatment of Personal Data, rectification or your relationship with us in general, please feel free to contact us at the following address: Embrace-IT ApS, VAT No. 36942320, Kildehøjvej 12, Dk-3460 Birkerød, Denmark, T: [+45] 45 3615 3600, E: info@embrace-it.com, www.embrace-it.com

12 Changes

12.1 We may change our Privacy Policy at any given time. You should review our Privacy Policy regularly. Such changes shall come into force immediately. If you do not agree to the modified Privacy Policy, please stop using our service. In the event of a conflict between this Privacy Policy and the modified terms, the modified terms shall apply. Your continued use of the services provided by us after the date the modified terms are posted will constitute your acceptance of the modified Privacy Policy.

13 Supervision

13.1 The Danish Data Protection Agency, inter alia, supervises the compliance with the applicable national regulation on Personal Data. The contact information for the Danish Data Protection Agency is:

Datatilsynet
Borgergade 28, 5
DK- 1300 Copenhagen K
T: 3319 3200
F: 3319 3218
E-mail: dt@datatilsynet.dk