PRIVACY POLICY

Travel Refund ApS

Date: 28 February 2020

1 RESPONSIBILITY

1.1 Protecting your Personal Data is our top priority, whether this data is about you, your transactions, your products/goods or your services.

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

2 COMPANY

2.1 The company is:

Travelrefund ApS
CVR Number: 39330571
Vestergade 20 C
DK-1456 København K
Danmark
(Hereinafter referred to as "Travelrefund")

T: + 45 82 82 85 85
Email: info@travelrefund.com
W: www.travelrefund.com

3 PERSONAL DATA

3.1 It is important to us that your Personal Data is kept safe and confidential. We have procedures in place for collecting, storing, erasing, updating and disclosing Personal Data to prevent unauthorized access to your Personal Data and to comply with applicable law.

3.2 We ensure fair and transparent data processing. When we ask you to make your Personal Data available to us, we will inform you of which Personal Data we process about you and for what purpose. You will receive information about this when your Personal Data is collected. We do not collect information that is not relevant to the matter at hand. If unnecessary information is collected, said information is immediately erased.

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

4 TYPES OF PERSONAL DATA

CUSTOMERS

- General Personal Data (e.g., name and/or username, address, e-mail, date of birth, gender, location, etc.)
- Contact details
- Traffic data
- Unique numbers of network devices
- CPR number
- Location data, name, reg. no., mobile no.
- Bank information
- CRM System, names, address, telephone no., email, areas of interest
- CCTV
- We do not process sensitive information on customers, unless this information is mistakenly entered by the debtor himself into our systems. If so, we will erase this information as soon as possible from our systems if they are not relevant.

EMPLOYEES

- Master data, general Personal Data (e.g., name and/or username, address, e-mail, date of birth, gender, profile picture, location, etc.)
- CPR number [Danish Personal Identification Number]
- Personal Data about immediate family
- Personal Data on education
- Testimonials
- Previous employment
- Current position

- Work duties
- Working hours and other official work-related conditions
- Personal Data on alary and taxes, general Personal Data (e.g., name and/or user name, address, e-mail, date of birth, gender, location, etc.), CPR number, Personal Data on the account number to which the salary will be paid (NEMKONTO)
- Personal Data on sick leave and illness and other leaves of absence from work
- Pension information, name, address, telephone number, e-mail, CPR No., name of spouse, name of children
- Traffic data on Internet usage
- Transaction data
- Unique number of network devices
- E-mails
- Social Personal Data
- Illness/disease-related Personal Data, medical certificate, name, address, telephone number, e-mail, leave of absence, storing [of Personal Data] for purposes other than reporting for unemployment benefits, or to Statistics Denmark
- Data on education/training
- Timesheet recording
- Exit interviews, behavioral data, information about other employees
- Criminal record
- Earnings statistics (Denmark Statistics), general Personal Data (e.g., name and/or user name, address, e-mail, date of birth, gender, location, etc.), CPR number, Personal Data on salary and taxes, Personal Data on absence/illness
- Employee performance review/staff development interviews, general Personal Data (e.g., name and/or user name), education data, performance information, including access to employees' turnover and timesheet recording, behavioral data, information about other employees

- Applications, general Personal Data (e.g., name and/or user name, address, e-mail, date of birth, gender, profile picture, location, etc.), CPR number, Personal Data on salary and taxes, education data, work experience, recommendations, references
- Personality test, name, address, telephone number, e-mail, personal characteristics
- Recruitment, general Personal Data (e.g., name and/or user name, address, e-mail, date of birth, gender, profile picture, location, etc.), personal characteristics, CPR number, Personal Data on salary, education data
- Pictures of employees – e.g., for marketing purposes
- Employer paid mobile phone, name, address, telephone number, e-mail, call history, anonymized telephone number of recipient of call, statement of truth
- Quality control
- Access control systems/guest list
- Claims management
- E-boks [electronic mailbox], emails from public authorities, CPR number, name, address, health information, traffic fines, court transcripts, work-related injuries
- Employee signature (only the administrator has access)
- CCTV

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:

CUSTOMERS

- Help and advice in connection with flight compensation
- Improving consultancy and other services
- Customizing communications and marketing to meet your needs

- Customizing business partners' communications and marketing to meet your needs
- Direct marketing activities
- Website optimization
- Implementation of an agreement or measures upon your request
- Compliance with legal requirements
- Legal claims

EMPLOYEES

- Implementation of an employment contract
- Managing your relationship with us
- Compliance with legal requirements
- Legal claims

6 THE DATA SUBJECT'S RIGHTS

6.1 Handling requests from the Data Subject

6.1.1 We take a centralized approach to handling Data Subjects' rights. However, the person responsible will rarely be adequately equipped, within the individual case, to be able to judge whether the Data Subject's request can/should be fully or partially met. The answer will therefore be given following a dialogue with the relevant case handler, who can account for the reasons for or against a request/objection being accepted, respectively.

6.2 Right of access

6.2.1 Pursuant to Article 15 of the General Data Protection Regulation, the Data Subject is entitled to be informed whether their Personal Data 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 In addition, the Data Subject has the right to access the following information:

- the purpose(s) of the processing
- the categories of Personal Data concerned
- the recipients or categories of recipient to whom the Personal Data has been or will be disclosed, in particular, recipients in third countries or international organizations
- where possible, the envisaged period for which the Personal Data will be stored or, if not possible, the criteria used to determine that period
- the right to request from the data controller, rectification or erasure of Personal Data or restriction of the processing of Personal Data concerning the Data Subject or to object to such processing
- the right to lodge a complaint with a supervisory authority
- where the Personal Data is not collected from the Data Subject, any available information as to the data's source

6.2.3 The Data Subject also has the right to be informed of the appropriate safeguards if we have transferred Personal Data to third countries.

6.2.4 In order to properly fulfill an access request, we must search all systems – including all databases, as well as all hardware and all removable media – and also scour all physical documentation kept on file and disclose the Personal Data recorded about the Data Subject.

6.2.5 Pursuant to the Data Protection Act, the right of 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 concerns of the subject.

6.2.6 We believe that this, among other things, will include information covered by our duty of confidentiality. The right of access will therefore not have an independent significance, as long as access to Personal Data is required, which is subject to confidentiality.

6.3 Data portability

6.3.1 Furthermore, pursuant to Article 20 of the General Data Protection Regulation, the Data Subject is entitled to receive the Personal Data concerning 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 also has the right to transmit this information to another data controller without hindrance from the company when the processing is based on consent

and the processing is carried out by automated means. If the Data Subject exercises this right to data portability, the Data Subject also has the right to have the Personal Data transmitted directly from one data controller to another, where technically feasible.

6.3.3 The right to data portability only includes information provided by the Data Subject and will only comprise automatic processing. Moreover, the right to data portability will be very limited if the company bases its right to process Personal Data on a basis other than consent.

6.3.4 We believe that the right to data portability can only be applied to a very limited extent in relation to our customer information.

6.4 Right to rectification

6.4.1 Pursuant to Article 16 of the General Data Protection Regulation, the Data Subject has the right to obtain from the data controller, without undue delay, the rectification of inaccurate Personal Data about himself. In addition, taking into account the purposes of the processing, the Data Subject shall have the right to have incomplete Personal Data completed, including: 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. For example, the fact that we may have decided that a customer does not have legal basis to conduct a case is not personal information that can be rectified simply because the customer does not agree. Our assessment of the evidence must also not be rectified because the counterparty may not agree with our interpretation.

6.5 Right to erasure ('right to be forgotten')

6.5.1 Pursuant to Article 17 of the General Data Protection Regulation, the Data Subject is entitled to have his or her Personal Data erased by the company without undue delay. If we receive a justified request for this, then we have the obligation to the 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 to comply with a legal obligation or to establish, exercise or defend legal claims, cf. Article (17)(3) points (b) & (e).

6.5.3 We believe that the "right to be forgotten" will very rarely be relevant in relation to our case processing. It may become relevant, for example, if the Personal Data was not at all necessary for the processing of the case, and therefore should not have

entered into the case at all, or if the Personal Data is no longer necessary for the processing of the case. In that case, the obligation to erase the 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 any possible legal claims by customers.

6.5.4 If, pursuant 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 or data processors of the Data Subject's request for erasure of any links to or copies or reproductions of the Personal Data in question.

6.6 Right to object

6.6.1 Pursuant to Article 21 of the General Data Protection Regulation, the Data Subject is entitled, at any time, 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 general Personal Data if the processing is necessary to perform a task carried out for reasons of public interest or if the processing is necessary to pursue a legitimate interest and the interest of the Data Subject does not exceed that interest.

6.6.2 If an objection is filed, we will no longer reserve the right to process the Personal Data in question unless we can prove substantial legitimate reasons for the processing which supersedes the Data Subject's interests 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 of Personal Data because our processing can, to a large extent, be linked to the legal basis for establishing a legal claim, just as we – if the processing otherwise complies with the basic processing provisions – 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 civil rights and legitimate interests.

6.7 Right to restriction of processing

6.7.1 Pursuant to Article 18 of the General Data Protection Regulation, the Data Subject is entitled to have the processing of their Personal Data restricted if:

- the accuracy of the Personal Data is contested by the Data Subject, for a period enabling the data 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 its use instead
- the data controller no longer needs the Personal Data for the purposes of the processing, but it is required by the Data Subject for the establishment, exercise or defense of legal claims
- the Data Subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the data 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 We believe that this provision will only have limited importance for our access to process Personal Data as part of our case work.

6.7.5 In addition, the provision largely supplements our own independent obligation to continuously ensure compliance with the fundamental rights of the Data Subject.

7 GENERAL PROCESSING PRINCIPLES

7.1 PROCESSING PRINCIPLES

7.1.1 We will process Personal Data legally, reasonably and in a transparent manner in relation to the Data Subject.

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, and

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 unauthorized or unlawful processing and accidental loss, destruction or damage, by using adequate technical or organizational measures

7.2 Risk analysis

7.2.1 In connection with our case work we must carry out adequate technical and organizational 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) large-scale processing of sensitive information or of Personal Data relating to criminal convictions and offenses, or

b) systematic and extensive assessment of personal matters 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

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

7.3.4 We believe 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 The assessment finds, among other things, support in the preamble of the General Data Protection Regulation. According to recital 91, the processing of Personal Data should not be considered comprehensive by the impact assessment regulations in the case of a physician, health professional or debt recovery as relates to the processing of Personal Data about patients or customers.

7.3.6 If an impact assessment is carried out anyway, the result of the assessment will be taken into consideration when taking appropriate measures to address any increased risk to the rights and freedoms of natural persons.

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 the processing of Personal Data is included as our "core activity".

7.4.2 It is not our core activity to carry out large-scale processing of Personal Data or to carry out regular and systematic monitoring of individuals.

7.4.3 The Danish Data Protection Agency [Datatilsynet] stated in its "Guide on Data Protection Officers" that companies that process Personal Data as a secondary activity are not obliged to appoint a Data Protection Officer.

7.4.4 Our processing of Personal Data is considered to be a secondary activity.

7.4.5 We have therefore chosen not to appoint a Data Protection Officer.

7.5 In such cases, we believe that it is not necessary to appoint a DPO.

7.6 Transfer to social networks

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

7.7 Other transfers

7.7.1 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.

7.7.2 If we are forced to seek additional legal assistance, or if we need to file your case againt the airline for collection, your personal information will be disclose to the attorney and/or collection agency, provided that this is necessary.

7.8 Profiling

7.9 We do not use your Personal Data for profiling.

7.10 General technical measures

7.10.1 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:

7.10.2 Access to Personal Data is restricted to persons who have a material need for access to Personal Data. 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. Within the company, all case managers have access to all cases. We have considered this to be necessary as all employees in the company are involved in the case processing.

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

7.10.4 Personal Data on paper – for example in records and binders – must be kept locked when not in use.

7.10.5 When documents (papers, filing cards, etc.) with Personal Data are discarded, shredding and other measures must be used to prevent unauthorized access to Personal Data.

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

7.10.7 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.

7.10.8 If the password is not renewed, access to the system is thereby closed.

7.10.9 If Personal Data is stored on a USB key, the 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. No Personal Data must be left on the employee's computer [laptop] desk. PCs connected to the internet must have an updated firewall and virus control installed.

7.10.10 When connecting to Wi-Fi, for free access, we ensure appropriate security measures taking into account the current state of technology development in the IT-area.

7.10.11 If website forms are used where sensitive Personal Data or personal identification numbers can be entered and submitted, encryption must be used.

7.10.12 If sensitive Personal Data or personal identification numbers are sent by e-mail via the internet, such e-mails must be encrypted. Insofar as possible, we strive to omit the last 4 digits of the CPR [Personal ID No.]. However, if it is considered that the last 4 digits of the CPR are absolutely necessary, the email is then encrypted.

7.10.13 In connection with the repair and servicing of computer equipment containing Personal Data, the necessary measures have been taken by not including Personal Data so that unauthorized persons cannot gain access to said information. The aim is that no Personal Data is stored outside the systems designed for this purpose, unless this is necessary for the case work.

7.10.14 In the situations where a computer is sent for repair and where Personal Data is stored on said computer, we establish several passwords [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, agreement and verification should ensure that repairers do not unduly access Personal Data, for example, by using confidentiality statements.

7.10.15 When using an external data processor to handle Personal Data, a written data processing agreement is signed between us and the data processor. This applies, for example, when using an external document archive or if cloud systems are used in the processing of customers' Personal Data – including communication with the customer.

7.10.16 We protect your Personal Data and have internal information security rules. We have adopted internal information security rules that contain instructions and measures which protect your Personal Data from being destroyed, lost, or modified, from unauthorized disclosure, and against unauthorized access or knowledge of them.

7.10.17 We will ensure that collected Personal Data is processed carefully and protected according to applicable safety standards.

7.10.18 We have strict security procedures for collecting, storing and transferring Personal Data to prevent unauthorized access and compliance with applicable laws. Our security is regularly checked. The Personal Data and sensitive Personal Data you provide us are stored on our own or on one of our data processor's servers.

7.10.19 We have taken the necessary technical and organizational safeguards to protect your Personal Data from accidental or unlawful destruction, loss or alteration and against unauthorized disclosure, misuse or other actions contrary to applicable law.

7.10.20 We store and process your Personal Data on IT systems with controlled and restricted access. The systems are located on servers in secured premises.

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

7.10.22 If you send Personal Data to us via email, please note that sending to us is not secure if your emails are not encrypted.

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

7.10.24 We have full access to all your Personal Data stored in our database(s) and on our server(s). Data will only be accessed on a "need to know" basis.

7.11 Backup

7.11.1 We back up all databases and files on shared drives every night. The backup is stored partly on an internal server and partly on an external data center.

7.11.2 We make the following types of backups:

- 1) 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 (this backup is goes back daily).

- 2) Clone backup. This backup strategy creates a perfect copy of each device on the network (this backup goes back 7 days)

- 3) Offsite backup. This backup safeguards against data loss if the backup is stored on site. All data and files are backed up and the backup is stored offsite.

7.11.3 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 the live environment, but will remain on the 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". We reload in terms of provisions regarding erasure. The person who wants to be erased will be erased.

8 PROCESSING RULES – CUSTOMER

8.1 General Information

8.1.1 Processing rules – Customers are intended as the general principles, which we must use in case work for customers and are thus a review of the issues that we generally have to deal with in our case processing. Processing rules – Customers are also an expression of how we meet the documentation requirements of the General Data Protection Regulation.

8.1.2 Employees are instructed to make data minimization of e-mails that are located in Outlook.

8.1.3 Based on the present processing rules – customers take the subject-specific processing rules into issues that are particularly evident in the relevant subject-specific areas.

8.2 Data Controller

8.2.1 We predominately work according to instructions from and dialogue with the customer. In relation to clients, other third parties and employees, we work as independent data controllers. As a Personal Data controller, we independently assess whether there are grounds for collecting/processing Personal Data, which Personal Data is relevant and necessary, and how long the Personal Data must be stored.

8.3 Data Processors

8.3.1 If third parties are involved in the case processing, we must assess whether such third parties receive the status of data processors or independent data controllers.

8.3.2 An example of the transfer of Personal Data to a third party is a situation where we make a request to another debt collection agency or lawyer for assistance in resolving a case. In such a situation, the other collection agency/law firm, as the main rule, will be considered to be a data controller for us.

8.3.3 In cases where this is not a data processor arrangement, the party receiving the information from us will be responsible for the subsequent processing of the Personal Data.

8.3.4 As stated above, when transferring data to an independent data controller, it must be ensured that there is a legal basis for the disclosure, and the receiving party must ensure fulfillment of its duty of disclosure.

8.4 Data processing agreement

8.4.1 In cases where we are data controllers and have considered the existence of a data processor arrangement, a data processing agreement must be prepared.

8.4.2 The data processing agreement must be concluded between us (the data controller) and the other party (the data processor) and must comply with the General Data Protection Regulation's requirements for data processing agreements, cf. Article 28(3). This means that a contract or other legal document binding on the data processor must be prepared. It is also a requirement that the data processing agreement is in writing, including electronic form.

8.4.3 Furthermore, the General Data Protection Regulation sets out several specific requirements for the contents of the data processing agreement. The agreement 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 data 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.

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

8.5 Transfer to third countries

8.5.1 When using a data processor, obtaining a response from a law firm outside the EU/EEA or by communicating with counterparties, we must be aware that the transfer of Personal Data to a data processor or the transfer of Personal Data to another data controller outside the EU/EEA will imply that processing takes place outside the EU/EEA.

8.5.2 The General Data Protection Regulation requires the processing of Personal Data does not take place in countries with lesser data protection than the level of data protection in the EU, as provided for in Articles 44 to 49 of the General Data Protection Regulation.

8.5.3 As the starting point (Articles 44-47), transfer to countries outside the EU/EEA requires:

- that the EU Commission has approved the country (including the Privacy Shield for the United States),
- that we, the company, and the third party have entered into an agreement using the EU Commission's standard model clauses, or
- that there is an adequate level of protection established by approved binding company rules

8.5.4 In addition, some transfers can take place if:

- there is consent
- the transfer is required for the performance of a contract, or
- the transfer is required in order to establish, exercise or defend a legal claim

8.5.5 Regardless of the legal basis, a transfer presupposes that four basic guarantees are always fulfilled, cf. the Danish Data Protection Agency's "Guide to Transfer of Personal Data to Third Countries":

- Authorities in third country's access to and use of Personal Data from the EU must be based on clear, precise and accessible rules.
- Authorities in third country's access to and use of Personal Data from the EU must be necessary and proportionate (balance between purpose (national security) and intervention of Data Subjects' right to privacy protection).
- There must be an independent and efficient supervisory authority in the third country.

- There must be available and effective legal means for the Data Subjects in the third country.

8.6 Data processors – overview

8.6.1 We use external companies to carry out the technical operation of the company. These companies act as data processors of the Personal Data for which we are the data controller.

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

8.6.3 The data processor acts solely under our instruction.

8.6.4 We use the following data processors:

Data Processor	Location	Agreement Type
Sentia	Denmark	
Inventio	Denmark	
Gmail [Google mail]	EU	
Google Analytics	US	
Microsoft	EU	
Visma	Denmark	
Dataløn	Denmark	
Hornskov Vindberg	Denmark	

8.6.5 The data processor has taken the necessary technical and organizational security measures to ensure that the Personal Data is not accidentally or unlawfully destroyed, lost or impaired and that it does not become known to unauthorized persons, is misused or otherwise processed in a manner that violates data protection legislation. 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 organizational security measures.

8.7 Authority to process

8.7.1 Our authority to process Personal Data is primarily based on the relationship to our customer/client. In general, we will have the authority to process the necessary data within the framework of this task. This specifically follows from Article 6(1) (a) to points (c) and (f) and Article 9(2), points (a) and (f) of the General Data Protection Regulation.

8.7.2 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.

8.7.3 We are authorized to process personal identification numbers, (i) when required by law, (ii) if there is consent, or (iii) if it is necessary to establish a legal claim cf. § 11, cf. section 7 of the Danish Data Protection Act.

8.7.4 We believe that our processing of Personal Data, with respect to a customer, to a wide extent, will be permitted in the stipulated provisions.

8.7.5 We will carefully consider, in each case, what the task involves when processing Personal Data so that the individual employee fails to process – including recording and saving – Personal Data that is not relevant to the case. We must therefore, in all contexts, relate to the task's framework and ensure that no Personal Data is collected and processed which is not relevant. In particular, it is important to ensure that no Personal Data is processed on third parties that are not relevant to the case.

8.8 General principles – case processing

8.8.1 When starting the case, we must first and foremost make sure that the legal basis is clear – i.e., which data processing the task requires and that we have a legal basis for this.

8.8.2 Subsequently, we have to decide on our obligation, on our own initiative, to inform the customer of the processing we will be carrying out.

8.8.3 During the process, we must continually ensure that the collection and disclosure of Personal Data takes place in accordance with the purpose, and we must continuously consider our relationship with any data processors. If a third country is involved in the case, we must be aware of the specific rules governing the transfer of Personal Data to third countries.

8.8.4 Once the case is completed, we will decide how long we need to keep the information and when to erase it.

8.8.5 As a rule, we must avoid basing our processing of Personal Data on the consent of the customer. In fact, consent can be revoked and, moreover, does not give independent opinion next to the task/agreement on assistance.

8.9 Duty to disclose information – customers/counterparties

8.9.1 The duty to disclose information applies both to the customer, in relation to counter-parties and in relation to any other third parties who are assumed to be involved in the case processing. The duty to notify third parties must always be considered in relation to our duty of confidentiality, but the duty of confidentiality can unlikely, as a general principle, exempt from a duty to disclose information in all contexts. This requires a specific assessment and decision.

8.9.2 In relation to the customer, the duty to disclose information is fulfilled by sending a link to our privacy policy in the welcome letter describing the conditions for the co-operation.

8.9.3 Reference is made to the Privacy Policy in the communication:

- Our processing – including electronic and physical processing/storage and possible use of a cloud system and case processing system.
- Other relevant actors
- Storage period after completion.
- Rights and opportunity for appeal as well as the possibility of revoking consent if the data processing is to be based on consent. As far as the person's rights are concerned, it is clear from Article 21 of the General Data Protection Regulation on the Data Subject's right to object that the Data Subject should be made explicitly aware of that right and that this must be done not later than at the time of the first communication, cf. Article 21(4). The information must be communicated clearly and separately from other information.

8.10 Duty to disclose information – third parties

8.10.1 Third parties can, e.g., constitute counterparties or minor characters.

8.10.2 Pursuant to Article 14(5) point (d) of the General Data Protection Regulation, the duty to disclose information does not apply if the Personal Data must remain confidential due to the duty of confidentiality.

8.10.3 As long as the processing of Personal Data concerning third parties is involved in the case work, and as long as the data is covered by our duty of confidentiality, we do not have a duty to disclose information to such third parties.

8.10.4 However, the duty to disclose information takes effect as long as there is no longer a duty of confidentiality. We are continuously considering to what extent one can refrain from providing information with reference to his duty of confidentiality.

8.10.5 Pursuant to Article 14(5) point (b) of the General Data Protection Regulation, the duty to disclose information does not apply if it requires excessive effort to fulfill it. This exception has in practice been interpreted in such a way that does not include minor characters. These may be names of doctors and various other therapists, as well as names of various consultants, colleagues, neighbors and others who may be included in the description of the case, but where it is, for example, the function and not the person that is relevant, and where the identity of the person has no bearing on the matter and will not have any significance. The exception, however, presupposes that only contact information and corresponding general Personal Data about the person(s) in question are included.

8.11 Continuous collection and disclosure of data

8.11.1 The purpose is to solve the customer's case – to complete the task. Therefore, in the course of action that we take, we must ensure that the collection and disclosure of Personal Data only takes place insofar as the collection/disclosure is within what is necessary to resolve the customer's case.

8.11.2 When collecting Personal Data on the case, we must pay close attention to whether the data contains Personal Data about third parties who are not aware that you are processing Personal Data about the persons concerned. It may trigger the duty to disclose information to those concerned about the data processing taking place.

8.11.3 It is important that we simultaneously consider the necessity of entering Personal Data about the third party in question in the case. If not, the Personal Data should be erased immediately. This also avoids having to be subject to the duty to disclose information, etc.

8.12 Erasure – when

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

8.12.2 However, several other considerations and special provisions mean that Personal Data should not or cannot be erased until a certain number of years have passed.

8.12.3 The period in which the Personal Data is stored before erasure must be decided.

- 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.

- 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.

8.12.4 As a general policy (and unless otherwise specified in this Privacy Policy), all Personal Data for a specific case must be erased 10 years after the case ends. All information regarding a customer must be erased 10 years after the termination of the customer relationship, given that no relevant information is erased.

8.13 Erasure – how

8.13.1 According to the IT security text ST3 from the Danish Data Protection Agency regarding the erasure of Personal Data, the erasure of Personal Data means that Personal Data is irrevocably removed from all storage media on which it has been stored and that such 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 backups.

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

8.13.3 In addition, all correspondence, etc., from Outlook must be transferred to the electronic case and erased from Outlook, and all statements/presentations, etc., on various portable media and local drives must be transferred to the electronic case and otherwise erased.

8.13.4 This allows for the entire case to be erased from the electronic case system after the storage period has ended.

8.13.5 In a case where all of the Personal Data about a customer, and not just a specific case, must be erased, the electronic form with the customer's master data must be erased from the system, and the corresponding records, concerning the client, in all other systems must be erased.

8.13.6 Alternatively, Personal Data may be completely anonymized resulting in it not being able to be ascribed to a specific person. In this case, the General Data Protection Regulation does not apply and complete anonymization is therefore an alternative to erasure. It is, however, important to remember that anonymization, as an alternative to erasure, is conditioned upon erasure of all traces that may lead to the person to whom the data relates. This is often a very difficult task.

8.13.7 Following erasure/anonymization, 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.

8.14 IP addresses and browser settings

8.14.1 For each visit to our website, the IP address and browser settings you use are registered. Your IP address is the address of the computer you use to visit the website. 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 the website can always identify the computer used in case of abuse or unauthorized use in connection with the visit to or use of the website. The IP address is also used to determine your approximate location (at city IP-address level).

8.15 Demographic Personal Data

8.15.1 In connection with the posting of Personal Data, including personal sensitive Personal Data, on our website, we will log your demographic location. This Personal Data will be published along with the Personal Data you have posted on your profile.

8.16 Newsletter

8.16.1 If you subscribe to our newsletters, your Personal Data will be registered directly with us. If you no longer wish to receive newsletters from us, you can unsubscribe by logging into your profile and editing your Personal Data.

8.16.2 Contact information will be erased regularly. E-mails that may be important for determining a legal claim shall be stored for 5 years and then erased, unless legal claims have been raised, or are intended to be raised by us.

9 PRECESSING 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 a party or for the purpose of carrying out measures that are taken 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 employment

9.2.1 Prior to hiring an employee, we will process some general 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 general Personal Data, which is processed for the purpose of selecting an employee for our company, is Article 6(1), point (a) of the General Data Protection Regulation, 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 beyond 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 first 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 certificate of criminal record/police clearance certificate (private certificate of criminal record/police clearance certificate from

police records), but we can also obtain it with the employee's consent (private certificate of criminal record/police clearance certificate 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. Insofar as we request an employee to obtain a certificate of criminal record/police clearance certificate, we will only ask to see it, but not keep a copy for our records. If we request the employee to obtain a certificate of criminal record/police clearance certificate, or we, upon receiving your consent, obtain said certificate of criminal record/police clearance certificate, your consent is required for us to process the Personal Data.

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 authorized 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. By its very nature, 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 general Personal Data. However, a personality test may also include sensitive Personal Data. In that case, we require your explicit consent in order to process such 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 your health information, 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 after the termination of the employment relationship.

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, in some cases, we will request your consent to store your Personal Data collected during the recruitment process for a period of 3 years for use in similar recruitment 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, the 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 general 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 sick leave and sickness periods. In addition to this, we will carry out an independent collection of Personal Data about you. This may comprise, e.g., Personal Data which is registered on an on-going basis from managers and other employee (including minutes of performance reviews) and business partners. Any inquiries or complaints 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 [SKAT] 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. The 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 your health information, 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 outcome of personality tests do not necessarily contain sensitive Personal Data.

9.3.5 In general, we do not wich 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 insofar as it is necessary in accordance with § 56 of the Sickness benefit Act, without obtaining consent. In such cases, we will process sensitive 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 labor law or specific rights which comprise all types of obligations and rights based on labor 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 Processing of Personal Data about former employees, including erasure

9.4.1 We must erase Personal Data without undue delay. This may be relevant in, e.g., cases where Personal Data is no longer necessary to fulfill 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 termination 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., a labor law case. In such cases, Personal Data may be stored for as long as it is necessary to conduct the case. Correspondingly, this may apply in connection with occupational injuries.

9.4.3 In connection with the termination/resignation of an employee, there may be doubts about when we may transfer the Personal Data in our possession. Any transfer of references 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 general 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 the Personal Data is collected, 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 of disclosure does not apply if the employee is already familiar with the Personal Data.

9.5.2 In another 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 employee's 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 information about the other purpose and other relevant additional Personal Data about, e.g., deadline, insight, erasure, etc., prior to this further processing. The duty of disclosure ['duty to disclose information'] does not apply for several cases, including if the employee is already familiar with such Personal Data.

9.5.4 Job applicants will be informed if we carry out credit checks with credit bureaus and about possible storage of the credit information, including information stating in which cases Personal Data is stored.

9.6 E-mail

9.6.1 We allow for the use of e-mail and the internet available at the workplace. For this purpose, the employee has been assigned a special e-mail account.

9.6.2 Use of e-mail in a non-occupational context may only take place insofar as it is compatible with the employee's performance of the daily work for the company and in compliance with those guidelines. Non-occupational use should therefore be very limited.

9.6.3 We allow 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.

9.6.4 We consider all results and out come from the use of the company's IT equipment as our property, unless such results or outcome are clearly labelled with the word "private". This also applies to your documents and e-mails. This means that personal e-mails sent/received via your work e-mail may, in principle, be read by others.

9.6.5 We may review this Personal Data to enable us to pursue legitimate interests – such as the operation, security, restoration, and documentation considerations, as well as the use of controls – and the consideration of employees does not exceed those interests. In order to ensure compliance with the IT Security Guidelines as well as to prevent or remedy system crashes, IT officers can open any email and receive executable files.

9.6.6 In case of absence, for example due to illness, vacation or after you have left the company, we may give a colleague access to the employee's folders and e-mail account.

9.6.7 We 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 the company, such e-mails will not be read by anyone other than the beneficial recipient. We do not want to read e-mails labelled "private", unless it is clear from circumstances that a specific e-mail, despite the label, is not private or has content that could be a breach of your obligations to us.

9.6.8 Upon your resignation – voluntarily or involuntarily – your e-mail account at with us 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 us. 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. Personal Data concerning your e-mail account will be removed as soon as possible from our website and other publicly available information sites. Only one or very few trusted employees will then have access to your e-mail account [until it is closed].

9.6.9 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 , or are intended to be raised by us. If an e-mail has general interest with regard to a later comparable project/assignment, it can be saved in an anonymous form beyond 5 years.

9.7 Internet

9.7.1 We allow for a reasonable level of private use of e-mails and the internet available at the workplace. Internet access can be used for searches that do not conflict with general ethical standards. More specifically, internet access must not be used for visits to websites whose content is of a pornographic, political, extremist or discriminatory nature in terms of race, gender, ethnic social origin or religion. Similarly, when using e-mail, the employee must not send material of the above-mentioned nature.

9.7.2 We do not perform systematic or 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, we reserve the right to monitor and review the individual employee's activities and stored data on the IT-system.

9.7.3 Registration for specific internet services, such as subscription services or portals, etc., may only take place upon prior agreement.

9.7.4 We use a firewall/log, 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 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 log used is used solely for system-related purposes.

9.7.6 We may review employees' use of the internet for technical and security reasons and for reasons concerning the need to control employees' use of the internet.

9.8 Home workplaces [telecommuting]

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, cf. below.

9.8.2 Home workplaces must meet the following requirements:

- A description of the encrypted connection used between the ad hoc workplace and the network used
- Use of two-factor approval
- Our internal instruction to our employees regarding home workplaces.

9.9 CCTV

9.9.1 TV surveillance (hereinafter CCTV) is generally used in hopes of preventing crime. There is CCTV at our locations and locations close by.

9.9.2 Surveillance is carried out on an ongoing basis. The CCTV is set up in such a way that it is only activated by motion sensors.

9.9.3 CCTV images can be archived and viewed online. Images will be erased automatically after 30 days, unless they have previously been handed over to the Police. With regard to recordings containing information on criminal offenses, these will only be stored briefly for the purpose of police reporting, and storage will be done on the condition that the police report is made as soon as possible. The recordings are handed over to the police in connection with the notification and are erased from the systems immediately thereafter. The recordings will be erased after a maximum of 30 days.

9.10 Disclosure

9.9.4 Documentation data may be disclosed or presented in accordance with the following guidelines:

- To the police in connection with crime and clarification thereof.
- According to law or by court order.
- For other purposes, when persons who are identifiable by the data have given written consent for extradition.

9.11 Processing

9.9.5 The subsequent processing of the Personal Data collected from the CCTV is subject to a proportionality principle. We thus ensure that the TV surveillance is carried out in such a way that it minimizes the violation of the individual's integrity, and that it is always taken into consideration whether the desired purpose can be achieved with less intrusive means than CCTV and recording.

9.12 Information

9.9.6 CCTV signs are set up on access roads to the area as well as premises under surveillance.

9.9.7 Employees are informed in writing about the CCTV surveillance. When the CCTV cameras are being set up, all employees are informed directly by the company via e-mail or by letter about the scope and purpose of the TV surveillance.

9.9.8 All newly hired employees are informed that parts of the workplace are under CCTV surveillance, as well as about the exact scope and purpose of said surveillance. The information is also included in writing in the welcome package/employee handbook.

9.9.9 For others who are in areas that are under CCTV surveillance, it may be said that, in terms of further notification to those persons, it is disproportionately difficult, practically impossible and most certainly highly resource-intensive to provide to each person who comes within the reach of the cameras. In addition, it has been assessed that a more detailed text containing this information, in connection with the signs, will not necessarily be noticed and read by the persons concerned.

9.13 Internal surveillance

9.9.10 Persons within the internal areas under CCTV surveillance will be recognizable in surveillance images.

9.9.11 For employees whose permanent work stations/workplaces are in the areas under CCTV surveillance, information on this, as well as on the exact scope and purpose of the surveillance, is included in the employee handbook.

9.9.12 The cameras are connected 24 hours a day, but the recording function is deactivated using a special key for the entrance door.

9.14 External surveillance

9.9.13 Our buildings, as well as adjacent buildings, are monitored externally. The cameras are motion controlled, which means that they only record when motion is detected within the camera's angle. As the cameras record movements around the clock, employees and others with access to the building complex are recorded if they are located where the cameras are set up.

9.9.14 The cameras point towards the facades and if there is a path, etc., within the camera angle, this area becomes "concealed".

9.10 Recording of phone calls

9.10.1 We may record phone calls if the other participants have consented to the recording thereof in advance.

9.10.2 Recorded phone calls are erased after of maximum period of 120 days.

10 COOKIES

10.1 We collect Personal Data about you in various ways in connection with the operation of our website. We collect Personal Data about you on the website and through your use of the website in two ways: Through 'cookies' and through registration and use of the website.

10.2 If we place cookies on your devices, you will be informed about the use and purpose of collecting data via cookies. Before placing cookies on your devices, we ask for your consent. However, necessary cookies to ensure functionality and settings can be used without your consent.

10.3 You can find more information on our website about our use of cookies and on how to erase or reject them. If you would like to revoke your consent, please see the instructions under our cookie policy.

10.4 What are cookies and similar technologies?

10.5 Cookies are small bits of information that the website places on your computer's hard drive, on your tablet, or on your smartphone. Cookies contain information that is used to streamline the communication between you and your web browser. The cookie does not identify you as an individual user but identifies your computer.

10.6 We use similar technologies that store and read information in the browser or device and utilize local devices and local storage, such as HTML 5 cookies, Flash and other methods. These technologies can work across your browsers. In some cases, the use of these technologies cannot be controlled by the browser, but requires special tools. We use these technologies to store information, which is used to ensure the quality of our services and to capture irregularities in the use of the website.

10.7 When you visit our website for the first time, you will automatically receive a cookie. A cookie is a small text file that is stored in your web browser and which registers you as a unique user. This cookie identifies our web server when you visit our website and records its use.

10.8 A cookie may contain text, numbers or, e.g., a date, but there is no Personal Data contained in a cookie. It is not a program and cannot contain viruses.

10.9 We use cookies to be able to customize and create content and services that match your interests and wishes. We also use cookies to run demographic and user-related statistics, and thus determine who visits our website. We only record anonymous information such as IP numbers, number of bytes sent and received, internet host, time, browser type, version, and language, etc.

10.10 What types of cookies do we use and for what purposes?

10.11 We use cookies for:

- Statistics, i.e. to measure the traffic on our website, including the number of visits to the website, which domains the visitor comes from, which pages they view on the website, and which overall geographical area the user is in.

- Improving functionality, i.e. to improve functionality and optimize your website experience and help you remember your username and password so you don't have to log in again when you return to the website.

- Integrating with social media, i.e. to allow you to integrate with social media, such as Facebook.

- Ensuring the quality of our services and preventing abuse and irregularities in the use of the same.

- Showing specific marketing on our website, which we think you will find interesting.

10.12 Third-party access

10.12.1 We provide access to our subcontractors to inspect the contents of the cookies set by the website. However, this information may only be used on our behalf and cannot be used for the third party's own purposes.

10.13 Third-party cookies

10.13.1 Our website uses cookies from the following third parties:

- Google Analytics: Used only at server level and for statistical purposes. You can reject cookies from Google Analytics by clicking here: http://tools.google.com/dlpage/gaoptout
- Facebook: set by Facebook.
- Twitter: Set by Twitter if you interact with the Twitter plugin or are already signed in to Twitter from another source for the purpose of interacting with them.

10.13.2 Most browsers allow you to delete cookies from your hard drive, block all cookies or receive a warning before saving a cookie. However, you should be aware that there may be services and features that you cannot use because they require cookies to remember the choices you make. We hope that you will allow the cookies we set as they help us improve the website.

10.14 How to delete cookies

10.14.1 You always have the option to delete cookies stored on your computer.

- Guide to deleting cookies in Microsoft Internet Explorer
- Guide to deleting cookies in Mozilla Firefox
- Guide to deleting cookies in Google Chrome
- Guide to deleting cookies in Opera
- Guide to deleting flash cookies – applies to all browsers

10.15 Google Analytics

10.15.1 We use Google Analytics to analyze how users use the website. The Personal Data that the cookie collects about your use (traffic data, including your IP address), is sent to

and stored on Google's servers in the USA.

10.15.2 Google Analytics sets two types of cookies: (a) A persistent cookie showing whether the user is recurrent, where the user comes from, which search engine is used, key-words, etc., and (b) session cookies used to show when and how long a user is on the website. Session cookies expire after each session, i.e. when you close your tab or browser. Google does not link your IP address to any other Personal Data Google holds on to.

10.16 Most browsers allow you to delete cookies from Google Analytics. Read more about Google Analytics' use of cookies.

10.16.1 By using our website you consent to us using cookies as described. If you no longer wish to consent to the use of cookies, you must opt out of the cookies by changing the settings in your browser.

11 CHANGES TO OR PRIVACY POLICY

11.1 We may change this Privacy Policy at any given time without notice.

12 QUESTIONS

If you have any questions regarding this Privacy Policy, our processing of Personal Data, rectification or your relationship with us, please feel free to contact us at the following address: Travelrefund ApS, Vestergade 20 C, DK-1456 København K, Danmark , T: +45 82 82 85 85 , E: info@travelrefund.com, W: www.travelrefund.com.

13 THE DANISH DATA PROTECTION AGENCY [DATATILSYNET]

13.1 You can lodge an appeal at the Danish Data Protection Agency about our collection and processing of your Personal Data:

Datatilsynet
Borgergade 28, 5.
1300 København K

Telephone: +45 3319 3200
E-mail: dt@datatilsynet.dk
www.datatilsynet.dk