IDT Retail Europe Limited

Privacy Notice

Effective and Updated as of May 25, 2018

1. Who we are

IDT Retail Europe Limited ("IDT") gathers and processes your personal data in accordance with this notice and in compliance with the relevant data protection regulations and laws. This notice provides you with the necessary information regarding your rights and our obligations, and explains how, why and when we process your data. We are committed to protecting the privacy of your data.

IDT acts as a data controller when processing your personal data, which means that we determine the purposes and means of the processing of your personal data collected by us. IDT is a company registered in England and Wales under company registration number 135555314. Our registered office and contact information is:

IDT Retail Europe Limited
44 Featherstone Street
London EC1Y 8RN
Email: legal-uk@idt.net
IDT's Representative: Amy Reynolds
IDT's Representative's Email: data_info@idt.net

2. Who this notice applies to

This notice applies to the following people:

- users and customers of our products and services in the EU, including our Boss Revolution branded products and services, whether purchased directly from us or through our websites, our app or at an authorized agent (collectively, the "Products");
- users and visitors within the EU of or to our websites, including the following websites (collectively, the "Websites"):

  www.bossrevolution.co.uk

  www.bossrevolution.de

  www.bossrevolution.es

- users of our Boss Revolution calling application (the "BR App") in the EU.

When we use the term "Services" in this notice it refers to the Products, the Websites and the BR App collectively.

You should also read the terms of service for each Service that you use, which can be found at the applicable Website or in the BR App. We may update this notice from time to time and you should review it periodically for changes. Any updated notice will be posted on the Websites and in the BR App.

3. Data we collect and how we collect it

IDT receives and collects both personal and non-identifying data from you when we provide you with our Services, when you install, access or use our Services and when you communicate with us. We may also collect personal data and non-identifying data about you from third parties. Personal data means information either on its own or in conjunction with other data that enables a specific person to be identified, but does not include "de-identified," "anonymous," or "aggregate" information, which is not otherwise associated with a specific person. Non-identifying data means data that by itself cannot be used to identify a specific person. We do not receive or collect any personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and we do not process genetic data or biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation. We will never collect any unnecessary personal data from you.

The personal data that we collect from you or about you is:

3.1 Data you provide. Depending on the particular Service you use, you may provide the following data directly to us:

- name;
- address, including country of residence;
- email address;
- mobile phone number;
- payment information, including credit or debit card details;
- birthdate;
- other personal information necessary to verify you and/or your phone number; and
- other personal information you provide to us for customer support purposes, surveys, promotions, sweepstakes or product feedback.

3.2 Data we collect from you. Depending on the particular Service you use, we may automatically collect the following data from you or your device:

- security code, password and login credentials;
- service related diagnostic and performance information, including how you use our Services, and performance logs;
- call records, frequently called numbers, and network traffic data;
- messages sent with our Services, including chats, photos, videos and voice messages;
- personal, phone or social network contact information;
- information about your device, including model, browser, operating system, platform type, application software, mobile network, device identifiers and numbers, and Internet connection speed;
- browsing, searching and buying activity;
- IP address;
- Websites visited and websites you come from and go to next;
- BR App feature usage and stored content;

- certain data on your device, including your contacts, the phone numbers in your mobile address book, favorite lists and other installed apps;
- device location data if you use our location features; and
- transactional data when you purchase a Product, including personal data about other people (*e.g.,* the recipient of your purchase of a Product).

3.3 Data provided by third parties. Depending on the particular Service you use, we may obtain the following data from the following third party sources:

- credit data from credit reporting agencies;
- transactional data when you purchase a Product, including receipts or data from app stores or third parties processing your payment;
- data from government, law enforcement and fraud prevention agencies;
- aggregate data from third party marketing and consulting companies that collect consumer data such as demographic and interest data (examples of this data include hobbies, sports, or pet owner);
- contact and other marketing lead data from third party marketing firms;
- other users of our Services may provide us with your email address or phone number through the purchase/use of a Service, our refer-a-friend programs, their mobile address book or social networking platforms; and
- other data and information from third parties that helps us operate, provide, understand, customize, support and market our Services.

4. How we use your personal data

4.1 General. IDT takes your privacy very seriously and will never disclose, share or sell your personal data without your consent, except as set forth in this notice or required to do so by law. We do not process your data in any way other than as specified in this notice and we retain your data only for as long as is necessary. Where you have provided us consent to receive marketing materials, you are free to withdraw this consent at any time.

IDT processes your personal data to meet our legal, statutory and contractual obligations and to provide you with our Services. More specifically, we process all the data we collect to help us operate, provide, improve, understand, customize, support, and market our Services. In addition, we process data for general, operational and administrative purposes, including maintaining your account, authenticating you and contacting you. As used in this notice the terms "process," "processing," "use," and "using" data include any operation or set of operations performed on personal data or on sets of personal data, including by automated means, such as collecting, recording, scanning, organising, evaluating, analysing, structuring, storing, adapting, altering, retrieving, consulting, using, combining, erasing or disclosing by transmission, dissemination or otherwise making available to our affiliates and to select third parties (as described in this notice). Sometimes we use automated means, including profiling, and other technologies to process your personal data (see Section 4.3). Profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, including to analyse or predict aspects concerning that natural person's personal preferences, interests and location.

4.2 Specific use of your personal data. More specifically, the purposes, legal basis and reasons for processing your personal data are detailed below:

How we use your data	Our legal basis	Our reasons for using your data this way
• To communicate with you about our terms, policies, and other important information regarding our Services • To manage our Services, including to help us operate, provide, evaluate, improve, monitor, customize, bill and support our Services • To verify your account and activity and investigate any suspicious activity or violations of our terms • To perform due diligence, credit and fraud prevention checks • To maintain accurate record keeping and data back up • To detect, investigate, report, and seek to prevent crime, fraud, abuse or illegal use of our Services or customer accounts • To manage risk for us and our customers • To comply with laws and regulations that apply to us • To obtain legal advice and/or defend IDT • To respond to customer service issues and complaints and seek to resolve them[1]	**Legal and Vital Interests of Data Subjects**	• Fulfilling our legal duties to our customers • Complying with regulations and legal requirements that apply to us • Providing, improving, understanding, customizing and supporting our Services • General, operational and administrative purposes, including customer service and audit functions • Risk management and compliance • Legal advice and defense
• To perform our obligations under our Service agreements with our customers, including providing Services and performing your transactions • To manage our relationship with you, including maintaining your account and authenticating you • To communicate with you about our terms, policies, and other important information regarding our Services • To manage our Services, including to help us operate, provide, evaluate, improve, monitor, customize, bill and support our Services • To verify your account and activity and investigate any suspicious activity or violations of our terms • To perform due diligence, credit and fraud prevention checks • To collect a debt • To troubleshoot Service issues	**Contract**	• Exercising our rights set out in agreements, arrangements or contracts (whether formal or informal) with our customers and vendors • Ensuring we provide the level of service that our customers expect, in line with any terms and conditions or contracts of service • Fulfilling our contractual duties to our customers • Complying with contractual requirements • Providing, improving, understanding, customizing and supporting our Services • General, operational and administrative purposes, including customer service

• To manage how we work with other companies that provide services to us and our customers • To respond to customer service issues and complaints and seek to resolve them[1]		
• To communicate with you about our terms, policies, and other important information regarding our Services • To manage our relationship with you, including maintaining your account and authenticating you • To manage our Services, including to help us operate, provide, evaluate, improve, monitor, customize, bill and support our Services • To verify your account and activity and investigate any suspicious activity or violations of our terms • To perform due diligence, credit and fraud prevention checks • To maintain accurate record keeping and data back up • To manage risk for us and our customers • To maintain and manage our customer database • To troubleshoot Service issues • To respond to customer service issues and complaints and seek to resolve them[1] • To detect, investigate, report, and seek to prevent crime, fraud, abuse or illegal use of our Services or customer accounts • To ensure the security of our network and information • To measure our marketing campaigns • To develop new ways to meet our customers' needs and to grow our business, including to research, test and develop new products and services for our customers • To perform product and organizational analysis, development and management, including financial management, audit functions and statistical analysis of our Services and customers • To provide industry analysis and demographic profiling	**Legitimate Interest**	• Ensuring we provide the level of service that our customers expect, in line with any terms and conditions or contracts of service • Fulfilling our contractual duties to our customers • Providing, improving, understanding, customizing and supporting our Services • General, operational and administrative purposes, including customer service • Providing our customers with a better Service experience • Improving the quality and value of our Services • Understanding how our Services are used • Sending you direct marketing information where we have assessed that it or may be beneficial to you as a customer and in our interests • To allow customers to participate in interactive features if they choose to do so • Tailoring a new product or service • Ensuring you always have the option to update your marketing preferences, allowing you to maintain complete control over what marketing information you receive

• To provide direct marketing identified as being beneficial to our customers and in our interests (subject to your marketing preferences)[2] • To create specific and tailored marketing, based on your activity, that is identified as being beneficial to you and in our interests (subject to your marketing preferences)[2]		

1. Where legally permissible, our communications with you, including phone conversations, chats and emails, may be monitored and recorded by us for quality assurance or for legal, regulatory or training purposes; you can opt out of this monitoring in advance.
2. You have the right to opt-out of receiving direct marketing materials from us. See Section 12 of this notice. Opting out shall not affect the lawfulness of processing before such opt-out.

4.3 Automated decision making. At times we will use systems to make automated decisions based on your personal data. This enables us to make quick and fair decisions, based on what we know. These automated decisions can affect the products, services, or features available to you. We use your data to make automated decisions mainly for (a) ecommerce risk management in order to spot any activity that could potentially be fraudulent or criminal and (b) to understand how you use our Services. If we think there is a risk of fraud or criminal activity, we may take action such as denying a transaction or refusing access to a Service or a feature of a Service. In addition, when you open an account with us we use automation to check that the Product is relevant for you, based on what we know. You have the right not to be subject to a decision based solely on automated processing that significantly affects you and you can request that we not make our decisions based solely on automated means – see Section 6.8.

4.4 Cookies and other web technologies.

(a) Cookies and web beacons. A cookie is a small piece of data sent from a website and stored on your computer by your web browser as a marker while you are browsing. When you visit a site that uses cookies for the first time, a cookie is downloaded onto your computer/mobile device so that the next time you visit that site, your device will remember useful information such as items visited pages. Cookies are widely used in order to make websites work more efficiently. Our Websites and the BR App rely on cookies to customize and optimise your experience and for features and services to function properly. Web beacons are used to tell us how and when pages in our sites are visited and to monitor performance of the Websites and BR App. Most web browsers allow some control to restrict or block cookies and beacons through the browser settings; however, if you disable them you may find this affects your ability to use certain parts of the Websites and BR App. By using the Websites or BR App, without adjusting your browser/phone settings, you are consenting to our use of cookies and web beacons.

These technologies collect non-identifying data only, not personal data. We do not honor any web browser "do not track" signals or other mechanisms that provide you the ability to exercise choice regarding the collection of data about your online activities over time and across third-party websites or online services. We use and share this data to deliver customized content and advertising, to ensure that you see the correct product information, to manage the frequency with which you see an advertisement, to tailor advertisements to better match your interests, and to understand the effectiveness of our advertising. The content may be delivered on the Websites, on non-IDT websites, on the BR App, by our representatives, and via email, SMS, push notification or other IDT services. In addition, if you respond to or interact with a particular advertisement, you may later receive a targeted advertisement as a result of an ad server or ad network concluding that you fit within a particular audience we are trying to reach.

The cookies we use may be session cookies (which are temporary cookies that identify and track users within the Websites and BR App and which are deleted when you close your browser or leave your session in the application) or persistent cookies (cookies which enable the Websites and BR App to "remember" who you are and to remember your preferences within the Websites and BR App and which will stay on your computer or device after you close your browser or leave your session in the application). Below is a summary of the cookies and beacons we use and why:

Cookie/Web Beacon Provider	Cookie/Web Beacon Type	Why we use
IDT	Strictly necessary	Required for the operation of the Websites and BR App, including permitting you access to secure areas of the Websites and BR App
	Functionality	To recognise you when you return to the Websites and BR App; to enable us to protect and authenticate access, to personalise our content for you, greet you by name, remember your preferences, make recommendations and complete transactions you request
	Functionality	To help keep users safe and secure; to protect visitors from spam and fraud by ensuring safety of personal data; to support anti-spam measures and prevent phishers, scammers, unauthorised log-ins and hacking
	Targeting	To record your visits to the Websites and BR App, pages visited and links followed; to tailor content, including advertising, on the Websites and BR App to your interests in accordance with your marketing preferences
Third Parties (*e.g.,* Google Analytics)	Analytical/performance	To collect information about how you interact with the Websites and BR App, including recognising and counting users, recording which sites users have come from and how they journey through the Websites and BR App. We use this data to analyse user behaviour in the aggregate, detect trends, improve the Websites and BR App and to help users to find content more easily.

(b) Web analysis. We use certain Google Analytics Advertising Features, including Remarketing and Demographics and Interest Reporting. Google Analytics is a web analysis service provided by Google that allows us to collect data about the traffic on our Websites through Google cookies and other identifiers, which enables us, among other things, to create user segments based on demographic or interest data and to deliver relevant advertising. Google utilizes the data collected to track and examine the use of our Websites and to prepare reports on the activities and share them with other Google services. Google may use the data collected to contextualize and personalize the ads of its own advertising network. You may be able to opt out of the Google Analytics Advertising Features through your browser ads settings or by visiting Google's Ads Settings page.

(c) BR App. We engage certain third parties who use mobile software development kits to passively collect data from users of the BR App. We use this data primarily to help us deliver personalized notifications and to identify you in a unique manner across other devices or browsers for the purposes of customizing advertisements or content.

(d) IT Applications. We use various informational technology applications within our organization to process and store personal data, including customer relationship management tools, marketing databases, and other platforms. The servers for these applications are located in the United States.

5. How we share your personal data

We will never disclose, share or sell your personal data without your consent, except as set forth in this notice or required to do so by law. We share all the information we collect and receive with our affiliates, both in and outside the EU, and to select third parties, to help us operate, provide, improve, understand, customize, support, and market our Services, and for general, operational and administrative purposes, including maintaining your account, authenticating you and contacting you. All third party data processors acting on our behalf only process your data in accordance with instructions from us and are required to comply fully with this notice, the relevant data protection laws and any other appropriate confidentiality and security measures. IDT does not sell your data to third parties without your consent. IDT does not sell, rent or lease its customer lists to third parties. Finally, you share your information as you use and communicate through our Services.

5.1 Data shared within the IDT family of companies. We share data within the IDT family of companies, including our affiliates both in and outside the EU, to operate, provide, support and market (subject to your marketing preferences) our Services. For example, if you purchase a Product, then we share your purchase information with various IDT affiliates in order to process your transaction.

5.2 Data shared with third parties. We share data with the following categories of third parties for the reasons stated below. We require that all these processors protect your data and limit their use of the data solely for the purposes for which it was provided. Moreover, we require that these processors comply fully with this notice, the relevant data protection laws and any other appropriate confidentiality and security measures. Finally, if you purchase products or services offered jointly by IDT and one of our partners, your personal data may be received by both IDT and our partner that is providing the product or service. For these jointly offered products and services, you should also review the partner company's privacy notice, which may include practices that are different from the practices described here.

(a) Business partners. We work with various retailer and distributor agents, vendors, professional advisors and partners for a variety of business purposes to help us offer, operate, provide, improve, evaluate, customize, and support our Services. We share data with these people solely to the extent reasonably necessary for them to perform work on our behalf. For example, we provide your data to our customer service vendor so that the vendor's agents can assist you when you call customer service.

(b) Advertising companies. We may share data with advertising companies to help us serve ads and market our Services. In addition, we also may share certain data, including email addresses and mobile phone numbers, with third party processors like Google or Facebook for marketing, advertising and analysis purposes, including the delivery of advertising campaigns and preparing and sharing aggregate business and marketing reports, demographic profiling and to deliver targeted advertising about our Products (subject to your marketing preferences). Often this data is non-identifying, anonymous and/or aggregated.

(c) Other processors. We may share data with other third party processors for various business and corporate functions, including risk management, compliance, operating, maintenance and hosting of our information systems and for data storage/backup/archive functions.

(d) Professional advisors. We may share data with our legal, audit and other professional advisors, including consultants and experts, for general corporate, financial and legal purposes.

5.3 Special Circumstances. We may share your data with various government, administrative and law enforcement agencies, regulators or other third parties in the following special circumstances:

- to comply with valid legal process including subpoenas, court orders, warrants, and as otherwise permitted or required by law;
- to assist law enforcement in cases involving national security, defence, public security, danger, death or serious physical injury to any person or in other emergencies;
- to assist law enforcement in the prevention, investigation, detection or prosecution of criminal offences, including the safeguarding against and the prevention of threats to public security;
- to protect our rights or property, or the safety of our customers or employees;
- to protect against fraudulent, malicious, abusive, unauthorized or unlawful use of our Services and to protect our network, Services, devices and users from such use;
- to advance or defend against complaints or legal claims in court, administrative proceedings and elsewhere;
- to prospective purchasers of all or part of our business or assets; and
- with your consent.

5.4 Data shared with third party advertising entities or social networks. You may see third party advertisements on our Products, the Websites and/or the BR App. Some advertisements are chosen

by companies that place advertisements on behalf of other third-party advertisers. These companies, often called ad servers, may place and access cookies on your device to collect data about your visit. The data they collect from our sites is in a form that does not identify you personally. This data may be combined with similar data obtained from other websites to help advertisers better reach their targeted audiences. Targeting may be accomplished by tailoring advertising to interests that they infer from your browsing of our sites and your interaction with other websites where these ad servers also are present. If you choose to interact with specific advertisers who advertise on the Products, the Websites or the BR App, the data you provide to them is subject to the conditions of their specific privacy notices. The Websites and BR App also include social network or other third party plug-ins and widgets that may provide data to their associated social networks or third parties about the website pages you visit, even if you do not click on or otherwise interact with the plug-in or widget.

5.5 When you share data. You share your data when you use and communicate through our Services. Your phone number, profile name and photo, and online status may be available to anyone who uses our Services, although you can configure your Service settings to manage certain data available to other users. Users with whom you communicate may store or share your data, including your phone number or messages, with others on and off our Services.

6. Your rights

6.1 General. IDT takes measures to protect your data and keep it private, but your privacy is also protected by law. Under the General Data Protection Regulation ("GDPR") you have certain access rights regarding your personal data and we are only allowed to use your personal data if we have a valid reason to do so. In addition, we comply with the data protection principles of the GDPR, meaning that your personal data is:

- processed lawfully, fairly and in a transparent manner;
- collected for specified, explicit and legitimate purposes as set forth in this notice and not further processed in a manner that is incompatible with those purposes;
- adequate, relevant and not excessive;
- accurate and complete;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
- processed in accordance with your rights;
- kept secure; and
- not transferred to countries without adequate protection.

6.2 Right of access. You have the right to access any personal data that IDT processes about you and to request information about:

- what personal data we process about you;
- the purposes of the processing;
- the categories of personal data concerned;

- the recipients, or categories of recipients, to whom the personal data has/will be disclosed, including recipients in any third country (in which case we will inform you of the appropriate safeguards relating to the transfer);
- how long we intend to store your personal data (or the criteria used to determine that period);
- the existence of other rights you have, including your right to request rectification of any inaccurate personal data held by us, your right to restrict the processing of your personal data or to object to such processing, and the right to data portability;
- your right to lodge a complaint with a supervisory authority;
- the source of any personal data about if that we did not collect directly from you; and
- the existence of automated decision-making, including profiling.

6.3 Right of rectification. You have the right to request rectification of any inaccurate personal data held by us. Where you notify us of inaccurate data about you, and we agree that the data is incorrect, we will amend the details promptly as directed by you and make a note on our system of the change and reasons. We will rectify any errors and inform you in writing of the correction and where applicable provide the details of any third party to whom the data has been disclosed. If for any reason we are unable to act in response to a request for rectification and/or data completion or need more time, we will provide a written explanation to you and inform you of your right to complain to the supervisory authority and to seek a judicial remedy. You may also correct or update your personal data, including changing your marketing preferences, by contacting IDT customer service by phone or email using the contact information contained in Appendix 1 to this notice or by accessing your account online and providing the updated data there.

6.4 Right of erasure (right to be forgotten). You have the right to request erasure of your personal data in certain circumstances, including where the including the data are no longer necessary to the purposes for which it was collected, you withdraw your consent (and there is no other legal basis for processing) or you object to the processing (and we have no overriding legitimated grounds for the processing). Even if you request erasure of your data, we may continue to hold and process such data under certain circumstances, including for compliance with legal obligations.

6.5 Right to restrict processing. You have the right to restrict processing of your personal data under certain circumstances (such as when the accuracy of the data is contested) and subject to certain exceptions (such as processing for legal claims).

6.6 Right to data portability. You have the right to data portability, meaning the right to receive the personal data concerning you which you have provided us in a commonly used, machine-readable format and to have that data transmitted to another controller (where feasible), if our processing is based on your consent or a contract and the processing is carried out by automated means.

6.7 Right to object to processing. You have the right to object to any processing of your personal data which is based on our legitimate interests, including profiling, and we shall no longer process such data unless we demonstrate compelling legitimate grounds to do so. You also have the right to object to the processing of your personal data for direct marketing purposes.

6.8 Right not to be subject to automated decision. You have the right not to be subject to a decision based solely on automated processing, including profiling, which significantly affects you, subject to certain exceptions including if the decision is necessary for us to perform our contract with you or is authorised by EU or Member State law or is based on your consent. At times we will use systems to make automated decisions based on your data. You can challenge these automated decisions, and ask that a person review the data and the result.

6.9 How to make a request. To make a request for access to your personal data or to exercise any of your other rights, you can email us at data_info@idt.net or visit our Subject Access Request page on the Websites. You can also submit your request in writing using the form in Appendix 2 to this notice and sending that form to us at:

IDT Retail Europe Limited
44 Featherstone Street
London EC1Y 8RN
Attn: Data Protection Team

6.10 How we handle requests. If we receive a request from you to exercise any of the above rights, we may ask you to verify your identity before acting on the request to ensure that your data is protected and kept secure. We are required to respond to your request within one month of receipt of the request. However, in certain circumstances, we may take an additional two months to respond. Where a request is received by electronic means, we will provide the requested information in a commonly used electronic form (unless otherwise requested by the data subject). We may be subject to EU or Member State law that restricts some of your rights primarily in order to safeguard national security, public defence, public security, the prevention, investigation, detection or prosecution of criminal offences, other important objectives of general public interest of the EU or of a Member State, the protection of judicial independence and judicial proceedings, the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions, the protection of the data subject or the rights and freedoms of others and the enforcement of civil law claims.

7. How we protect your personal data

IDT takes your privacy seriously and takes every reasonable measure and precaution to protect and secure your personal data. Our employees are trained on the importance of protecting your privacy and on the proper access to, use and disclosure of personal data. We work hard to protect you and your data from unauthorised access, alteration, disclosure or destruction and we have implemented technical, organizational and physical controls, safeguards and measures including:

- **Physical Access Controls** – to prevent unauthorized persons from gaining access to data processing systems and include secure areas and equipment security. Physical access rights and authentication controls for secure areas have been implemented and documented and will be regularly reviewed and updated by central functions. We secure data on computer servers in a controlled, secure environment.
- **Logical Access Controls** - to prevent data processing systems from being used without authorisation by way of personal login with a secure password that has to be changed periodically.
- **Data Access Controls** - to ensure that persons with system access authorisation have access only to those data they are authorized to process and use. A process has been established to ensure that data is accessed only by those persons who are required to gain

access for their work. Access is regulated by way of personal login with a secure password that has to be changed periodically.

- **Disclosure Controls** - to ensure that personal data cannot be read, copied, altered or removed without authorisation during electronic transfer or transport or while being recorded onto data storage media. State-of-the-art data transmission techniques are used that ensure (amongst other things) that it will be possible to check the recipient of the personal data transferred. Storage and transport precautions are taken to protect data media against damage or theft.
- **Input Controls** - to ensure that it is possible after the fact to check and ascertain whether personal data have been entered into, altered or removed from data processing systems and if so, by whom. Logs are regularly evaluated by the person responsible for the system.
- **Job Controls** – to ensure that personal data is processed strictly in compliance with our instructions. We take steps to ensure that any natural person or processor acting under our authority does not process data except on instructions from us (except as otherwise required by law).
- **Availability Controls** - to ensure that personal data is protected against accidental destruction or loss, for instance by way of regular updates and storing of data on separate computer equipment or storage media.
- **Separation Controls** - to ensure that data collected for different purposes can be processed separately by way of separating the access to the data.
- **Default Controls** – to ensure that we only process your data which are necessary for each specific purpose of the processing, that we wherever possible minimize the processing of your data and that we maintain transparency with regard to the functions and processing of your data.
- **Encryption Controls** – to convert data into a code to make your data unreadable by anyone who might intercept it and include using 128-bit encryption on our online pages that hold your data, the pseudonymisation of data and the use Secure Socket Layer (SSL) encrypted protection to protect data transmitted by you to the Websites and BR App. You can tell that SSL is in use when a small padlock icon appears on your browser status bar.
- **Industry Controls** – to ensure that our receipt and processing of certain payment data are in compliance with applicable industry regulations, *e.g.,* the Websites and BR App are PCI compliant in connection with your credit card data.
- **Monitoring Controls** – to enable us to constantly check the ongoing confidentiality, integrity, availability and resilience of our processing systems. We routinely test and evaluate the effectiveness of our technical and organizational safeguards and measures.
- **Your Online Security Controls** - on registering your personal data with us on the Websites or BR App you will be able to choose a username and password, allowing you to access certain restricted parts of the Websites and BR App. You must be responsible for protecting your own personal data, and we recommend that you keep your PC or device updated with anti-virus software, treat emails with caution (remember we will never ask you to disclose personal data via email) and ensure you choose a password that can not be easily guessed.

Although we work hard to protect your data, no program is 100% secure and we cannot guarantee that our safeguards will prevent every unauthorized attempt to access, use or disclose that data. The risks that may result from our processing of your personal data include identity theft or fraud, financial loss, loss of confidentiality, unauthorised reversal of pseudonymisation, and the inability to exercise control over your personal data. IDT maintains security and incident response plans to handle incidents involving unauthorized access to data we collect or store. If you become aware of an issue, please contact us.

IDT does not knowingly market to or collect information from children under the age of 13 without obtaining verifiable parental consent. If you allow a child to use your device or our Services, you should be aware that their information could be collected as described in this notice. We encourage parents to be involved in the online activities of their children to ensure that no data is collected from a child without parental permission.

8. Transfers of data inside and outside the EEA

Personal data in the EU is protected by the GDPR, but some other countries may not necessarily have the same high standard of protection for your data. We transfer data outside the European Economic Area to both our affiliates and certain third party vendors in the United States and other countries solely for the following purposes: website hosting; hosting of servers for informational technology applications, including customer relationship management tools and marketing databases; and fraud/risk management. Where this is the case, we will take steps to ensure that those affiliates and vendors use the necessary level of protection for your data and abide by strict agreements and measures to protect your data and comply with the relevant data protection laws. IDT entered into a data transfer agreement to govern international data transfers to its U.S. parent corporation IDT, Telecom Inc. This agreement contains the EU model clauses relating to such transfers.

9. Consequences of not providing your data

You are not obligated to provide us with your personal data. However, this data is necessary for us to provide you with our Services. Accordingly, we will not be able to offer some or all our Services to you and/or you will not able to use certain features or functions of our Services, without providing us with your personal data. In addition, we may need to collect personal data by law or under the terms of a contract we have with you. If you choose not to give us this data, it may delay or prevent us from meeting our obligations. It may also mean that we cannot perform services needed to maintain your Products, and could mean that we cancel a product or service you have with us. Any data collection that is optional will be made clear at the point of collection.

10. Legitimate interests

As noted in the *'How We Use Your Personal Data'* section of this notice, we often process your personal data under the legitimate interests legal basis. Where this is the case, we have carried out a thorough review and assessment to ensure that we have weighed and balanced your interests and any risk posed to you against our own interests and ensuring that are processing activities are proportionate and appropriate. Based on our assessment, we reasonably believe that our direct marketing processing activities do not pose a likely privacy risk or detriment to you or your data.

We use the legitimate interests legal basis for processing for the purposes and interests listed in the *'How We Use Your Personal Data'* section of this notice.

11. How long we keep your personal data

IDT retains your data for only as long as is necessary for the purposes described above in *'How We Use Your Personal Data'* and we have strict review and retention policies in place to meet these obligations. We are required under certain applicable tax laws to keep your basic personal data (name, address, contact details) for a minimum of six years after which time it will be destroyed unless required to be kept for other purposes. Where you have consented to us using your details for direct marketing, we will keep such data until you notify us otherwise and/or withdraw your consent.

12. How we market our services to you

IDT will occasionally send you by email and/or text (SMS) message direct marketing materials, including promotions and special offers regarding the Services you use and other Services, which have been identified as being beneficial to our customers and in our interests. We process your personal data for this purpose under the legitimate interests legal basis noted above in the *'How We Use Your Personal Data'* section of this notice. Such information will be relevant to you as a customer and is non-intrusive and you will always have the option to opt-out/unsubscribe at any time. If you would prefer *not* to receive the above mentioned marketing, please (a) call or email an IDT customer service representative using the contact information listed in Appendix 1 to this notice or (b) access your account online. Opting out shall not affect the lawfulness of processing prior to such opting out.

13. How you can limit our sharing of your personal data

You have choices about how we collect, use and share your personal data.

13.1 Email, text messages and push notifications. Marketing emails you receive from us will include an unsubscribe feature usually found at the bottom of the email that you may use to opt out of receiving future marketing emails. Marketing text and SMS messages from us also contain an opt-out feature that you can use to prevent future marketing text and SMS messages from us. You can opt out of receiving push notifications from us via the BR App by going to your device "Settings" and clicking on "Notifications," and then changing those settings for the BR App. Please note that you cannot withdraw your consent to receive certain in-BR App messages from IDT. Your ability to manage some of our Services could be limited if you withdraw your consent to receive text and SMS messages. IDT does not recommend using those Services without authorization to receive such messages.

13.2 Online information. You have choices about whether certain data collected on the Websites and BR App is used to customize advertising based on predictions generated from your visits over time and across different websites and apps. Similarly, many mobile devices offer controls you can set to limit the advertising use of data collected across mobile apps on your device. Please note that many opt outs use browser cookies or device controls and are specific to the device and browser you are using. If you buy a new computer, change web browsers or devices or delete the cookies on your computer, you may need to opt out again. In addition, ads you receive may still be tailored using other techniques such as publisher or device or browser-enabled targeting. You should check the privacy notices of the products, sites, apps and services you use to learn more about any such techniques and your options. You also can limit the collection of certain website data by deleting or disabling cookies and web beacons. Most browsers enable you to erase cookies from your computer hard drive, block all cookies, or receive a warning before a cookie is stored and disable web beacons. Disabling cookies or web beacons may

prevent you from using specific features on our Websites and other websites, such as ordering Products and maintaining an online account.

14. How you can contact us or lodge a complaint

IDT only processes your personal data in compliance with this notice and in accordance with the relevant data protection regulations and laws. We will always aim to collect and use your personal data in a way meets the highest data protection standards. We take any complaints about data protection very seriously. If you wish to contact us, raise a complaint regarding the processing of your data or are unsatisfied with how we have handled your data, you can contact us in writing or by email at:

IDT's contact information

IDT Retail Europe Limited
44 Featherstone Street
London EC1Y 8RN
Email: legal-uk@idt.net
IDT's Representative: Amy Reynolds
IDT's Representative's Email: data_info@idt.net

If you remain dissatisfied with our actions, you have the right to lodge a complaint with the applicable supervisory authority in your Member State. Here is the contact information for the supervisory authorities in the United Kingdom, Germany and Spain.

Supervisory Authority contact information – United Kingdom

Information Commissioner's Office (ICO)
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Telephone: 0303 123 1113 (local rate) or 01625 545 745 (national rate)
Fax: 01625 524 510
Email: enquiries@ico.org.uk

Supervisory Authority contact information – Germany

The Federal Commissioner for Data Protection and Freedom of Information
Husarenstraße 30
53117 Bonn
Telephone: +49 (0) 228-997799-0
E-Mail: poststelle@bfdi.bund.de

Supervisory Authority contact information – Spain

Spanish Agency for Data Protection
C / Jorge Juan, 6
28001-Madrid
Telephone: 901 100 099 - 912 663 517

Electronic office: http: // sedeagpd.gob.es/sede-electronica-web/

15. Other information

15.1 Links to and from non-IDT websites and content. The Websites and BR App may contain links to non-IDT sites. In addition, IDT or Boss Revolution branded content may be included on websites that are not associated with IDT. We have no control over these non-IDT sites and are not responsible for the content on these sites or platforms or the privacy notices and practices employed by these sites and platforms. We recommend that you review the notices and practices of the sites you visit.

15.2 Social Networking. Some of our Services may allow you to participate in blog discussions, message boards, chat rooms, and other forms of social networking and to post reviews. Please be aware that these forums are accessible to others. We urge you to not submit any personal data to these forums because any data you post can be read, collected, shared, or otherwise used by anyone who accesses the forum. IDT is not responsible for the data you choose to submit in these forums. If you post content to data sharing forums, you are doing so by choice and you are providing consent to the disclosure of this data.

15.3 Changes to this Notice. We reserve the right to make changes to this notice, so please check back periodically for changes. You will be able to see that changes have been made by checking to see the effective date posted at the beginning of the notice.

Appendix 1

IDT Customer Service Contact Information

United Kingdom

Customer service phone: 03307771374
Customer service Email: support@bossrevolution.co.uk
Customer site: https://www.bossrevolution.co.uk

Spain

Customer service phone: 917714036
Customer service Email: support@bossrevolution.es
Customer site: https://www.bossrevolution.es

Germany

Customer service phone: 03025558917
Customer service Email: support@bossrevolution.de
Customer site: https://www.bossrevolution.de

Appendix 2

Subject Access Request Form

Under the General Data Protection Regulation, you are entitled as a data subject to obtain from IDT confirmation as to whether we are processing personal data concerning you, as well as to request details about the purposes, categories and disclosure of such data.

You can use this form to request information about, and access to, any personal data we hold about you. Details on where to return the completed form can be found at the end of the form.

1. Personal Details:

Data Subject's Name:		**DOB:**	___ / ___ / _____
Home Telephone No:		**Email:**	

Data Subject's Address:

Any other information that may help us to locate your personal data:

2. Specific Details of the Data Requested:

3. Representatives *(only complete if you are acting as the representative for a data subject)*
***[Please Note:** We may still need to contact the data subject where proof of authorisation or identity are required]*

Representative's Name:		**Relationship to Data Subject:**	
Telephone No:		**Email:**	

Representative's Address:

I confirm that I am the authorised representative of the named data subject:

Representative's Name: _____ **Signature:** _____

4. Confirmation

Data Subject's Name: _____ [print name]

Signature: _____ **Date:** ____ /____ /_____

5. Completed Form

For postal requests, please return this form to:	***For email requests, please return this form to***:
IDT Retail Europe Limited 44 Featherstone Street London EC1Y 8RN Attn: Data Protection Team	data_info@idt.net