Privacy Policy for flookyapps Home Solutions Version 7.1, adopted on 31.10.2022
This privacy policy applies to all flookyapps Home Solutions and their related support services, including the creation of an individual account on flookyapps Central. The Anti-theft, Parental control, VPN services, flookyapps Box, Premium Services, Digital Identity Protection and flookyapps Identity Theft Protection have additional privacy policies which are detailed in Chapter 7.

The document explains the personal data we collect, how and where we may use it, how we protect it, who has access to it, with whom we share it, and how you may correct it.

1. General information

S.C. flookyapps S.R.L. (hereafter mentioned as flookyapps), with its official headquarters in 15A Sos. Orhideelor, Orhideea Towers Building, 9-12 floors, 6th District, Bucharest, Romania, registered in the Bucharest Trade Register with number J40/20427/2005, fiscal code RO18189442, e-mail privacy@flookyapps.com processes personal data in agreement with the European legislation on data protection (GDPR – Regulation EU 2016/679). Our Data Protection Officer can be reached at dpo@flookyapps.com, Phone: +923111907476

flookyapps offers data security products and services. Our goal is to ensure information and network security by providing quality products and services in these areas while also respecting privacy and personal data of customers, Internet users and business partners.

For this purpose, we collect only that personal data absolutely necessary for the specified purposes, on a best efforts basis. We do not sell your data. For the collected information and data, we strive to apply adequate solutions to anonymize them, or at least to pseudonymize them.

Our main principle applied to the data we collect is anonymization of all technical data that can be used by flookyapps only for the specified purposes below. In cases where perfect anonymization of technical data is not possible, the potential identification of a user could be possible only in very limited cases and only by highly skilled IT specialists.

Personal data according to the European legislation definition (GDPR - Regulation 2016/679) means:

any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

In this context, flookyapps processes personal data for the following main purposes:

To ensure network and information security by:

assuring correct and efficient operation of its products and services, according to the technical specifications, and for their improvement, including analyzing the reported IT security issues, delivering and customizing the related services to the user’s needs and developing new technologies;

support or counseling services for its users of flookyapps Home Solutions;

To conclude and perform the contract with the user, including preliminary steps in this direction;

To make statistical analysis and market studies;

To perform marketing activities for flookyapps's own needs.

2. Personal data collected

flookyapps may collect personal information from its users from its Home Solutions in three different ways:

directly provided by a user or a flookyapps Partner;

indirectly provided by its products or other sources, such as:

technical data sent by the flookyapps products installed by users

publicly available information from data leaks.

2.1. Personal data directly provided by a user/partner

a) Currently, you may buy or renew the flookyapps Home Solutions from an authorized partner, in which case the personal data collected with this activity is processed directly by that respective partner (which is a data controller for that data collection).

In certain countries, you may also buy flookyapps Home Solutions directly by us with an online sale. In these cases flookyapps will collect directly from you the necessary data for contracting with you (including payment), for fiscal obligations and certain technical data from your device (IP, browser info and a device identifier) for fraud prevention purposes.

The necessary data for payment is processed by:

the payment services provider Adyen.com, which is a data controller for data on your credit card payment data (which is actually encrypted in accordance with PCI DSS standards). flookyapps will never have access to your full credit card details;

PayPal, if you choose this method of payment, which is a data controller for all payment data, which takes place on their website.

b) When you create an account or login in flookyapps Central (which is mandatory to activate and manage your services), we might ask your name, surname and/or email address for management of your flookyapps products or services, to contact you with updates, notices, feedback messages and other types or transactional communications, for improvement of the information security of your devices, or to provide support.

c) In certain cases, when you download a trial version of our products, we will collect your email address, in order to have a contact method with you, to receive information such as updates, notices, feedback messages and other types or transactional communications or for improvement of the information security of your devices, or to provide support. We

reserve the right to verify the existence of that email address, as a security check and to prevent fraud.

d) In addition, when you access the Support Center, we may ask for a valid email address or a phone number to communicate with you in providing support. We use this data to contact you, for contractual purposes, providing a specific user with a license to use our products, for solving a request or complaint you addressed to us or for offering technical support. flookyapps may also ask for other data that may be considered personal data, if those are necessary for solving the information security problem you sought help for.

The legal basis for processing these data is performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract. The minimum data for creating an account with flookyapps are a name and email address; without them, it would be impossible for us to offer you our products and services. The minimum data for online sales are the mandatory fields in the checkout form, without providing them it would not be possible to buy the flookyapps products and services from us.

These data used for online sale or licensing information is kept for the duration of the contract, and five years after its expiration to be able to prove or defend any legal complaints on contractual issues.

The personal data processed in compliance with our tax and accounting obligations are collected on the legal basis when processing is necessary for compliance with a legal obligation. These data will be kept for a period of 10 years from 1st January of the year following the accounting period to which they relate.

We collect the technical data used for fraud prevention purposes for the legitimate interest or preventing fraud. In case your card supports 3D Secure 2, this information is collected by your issuing bank as a data controller, and we do not have access to it.

The data used for support services is kept for different periods, depending especially if the problem has been solved and the exact method of communication with the support services, but in no case the data will be kept for more than five years after the last communication took place. This period is necessary for flookyapps to be able to defend any legal complaints on contractual issues that may arise.

As regards the use of these data for marketing purposes, the legal basis we use is legitimate interest for marketing communications with users of our Home Solutions (based on Recital 47 of GDPR and Romanian law 506/2004, art 12 (2) that is implementing the EU E-privacy directive), unless those persons have opted out.

Whenever we note that we use legitimate interest as a legal basis for a specific situation, we rely on internal legal analysis on how we have balanced out the legitimate interest to the interests or fundamental rights and freedoms of the data subject. The analysis is updated if we decide to collect more data, for another purpose or there are new developments that require a new assessment.

We may use these data for marketing purpose for a maximum period of contractual duration, and five years after the contract is terminated, except if the data subject has opted out from these communications at any moment in time. After this period expires, the data will be deleted or anonymized.

2.2. Technical data sent by flookyapps product

- when you use flookyapps products it is possible to share with us some technical details, such as data for identifying the device (UUID), the infected URL you reported or an IP addresses. If you use a flookyapps product that integrates with your email server, some technical data of the infected files could be send to us, including data such as sender, recipient, subject or attachment. If you use one of our mobile flookyapps Solution, we may collect installed application information whenever scans are performed, to check against the latest threat information available and warn you if alleged malicious apps are found. In most cases, all these technical data may not lead to your direct or indirect identification, but in some very specific cases, computer specialists might be able to identify a specific user. Therefore, we treat all such information as personal data and protect it as such.

This technical data is solely used for the purpose of information and network security by correct and efficient operation of the products and services, according to the technical specifications, and their improvement, including by analyzing the reported security issues. This includes delivering and customizing related services. In addition, we may use this information for statistical purposes and improving the quality of our products.

The legal basis for processing these data is performance of a contract to which the data subject is part of.

These data are being stored for a limited period, depending on its usefulness for the current information security needs. Based on the current speed of technology, we will not need them for over 10 years from the day of the collection.

2.3. Collecting Data from publicly available information (data leaks).

In the recent years, an increasing number of companies' databases have been involved in incidents leading to user details becoming publicly available. We are constantly analyzing these situations and the public data leaks in order to identify if the exposed records can be used to improve the information security of our users.

We use this information exclusively for ensuring information security by notifying our users that their emails, passwords or other data might have been hacked in the past, so it is not safe to use them anymore.

The legal basis for this collection is legitimate interest of our users, of flookyapps and of any third party to ensure network and information security, by not using credentials that have already been hacked. We do this based on Art 6 (1) f of GDPR and explanations on legitimate interest for information security in Recital 49 of GDPR. These data are being stored for a limited period, depending on its usefulness for the current information security needs. The data subject may always ask us not to collect data about him from data leaks.

Based on the current speed of technology, we will not need them for over 10 years from the day of the collection.

3. Protecting the Personal data

As a leader in information security services, confidentiality and data protection are of vital importance for us. Access to the collected personal data is restricted only to flookyapps employees and data processors that need access to this information. All flookyapps information security policies are ISO 27001 and SOC2 Type2 certified.

flookyapps may use other companies to process the collected personal data. These companies are considered data processors and have strict contractual obligations to keep the confidentiality of the processed data and to offer at least the same level of security as flookyapps. Data processors have the obligation not to allow third parties to process personal data on behalf of flookyapps and to access, use and/or keep the data secure and confidential.

flookyapps may host or transfer personal data in the European Union (EU) or any other jurisdiction, which offers adequate level of personal data protection according to European Union standards (art 45 GDPR) or other appropriate safeguards, including Standard Contractual Clauses (art 46.2 GDPR).

Due to confidentiality obligations and security requirements, the specific information regarding the name and details for each processor used will be provided only to competent authorities.

We use the following types of data processors:

hosting services in EU and USA;

support channel communications in EU and USA;

e-commerce support providers in EU and USA;

marketing services (including email marketing) in EU and USA.

Access to certain sections of flookyapps websites is protected by a username and password. We recommend not revealing this password. flookyapps will never ask for your account's password via any kind of messages or phone calls. We advise not to disclose your password to anyone asking you to do so. If possible, we also recommend to log out of your online services account after each session. We also advice to close the browser window after navigating or using flookyapps services.

Unfortunately, transferring data over the Internet cannot be 100% secure. Consequently, despite our efforts to protect personal data, flookyapps cannot assure or guarantee the security of the information transmitted by the user until the information is on our servers. Any information you transmit is done on your own risk.

4. Who has access to personal data

In principle, flookyapps will not reveal any personal data about its users to third parties without the exceptions mentioned above.

Exceptionally, flookyapps may reveal personal data to:

4.1. Competent authorities, upon their legal request according to the applicable laws or when this is necessary to protect the rights and interests of our clients and flookyapps.

4.2. flookyapps may allow limited access to its Partners, which are presented on flookyapps's Partners webpage. Access will be allowed only to certain data related to its referred clients and just for fulfilling the contractual obligations between flookyapps and its Partner for selling or for support of flookyapps products. All Partners have strict contractual obligations to keep the confidentiality of data and to offer at least the same level of security as flookyapps. These Partners have the obligation not to allow third parties to access personal data processed on behalf of flookyapps.

4.3. flookyapps subsidiaries in your country may send some personal information to its main company - S.C. flookyapps S.R.L, in Romania.

In addition, when you use flookyapps Home Solutions or access flookyapps Central and you are asked to give information about yourself, you will reveal this information only to flookyapps. The only exception is when the information is offered in partnership with another service (for example online payment with the payment processors mentioned above or to create a flookyapps account with Facebook login, Google+ login, Microsoft login or Apple ID).

Each time when such a service is offered in partnership with another provider you will be properly notified. If you wish this data not to be accessed or used you can choose not to allow data transfer via this particular service.

If you choose to accept data sharing, it is important to mention that the service partners may have separate data collection and privacy policies. flookyapps has no control and cannot offer guarantees regarding all the legal aspects that these independent confidentiality practices entail.

5. How to correct personal data related errors

When you create an account on flookyapps websites or for one of our services, a confirmation email with your account details will be sent. The confirmation email will be sent to the email you supplied and it may describe the ways in which you can modify or delete the account you created. We advise you to keep this confirmation email since it contains useful information regarding access to our services. Any requested modification will be solved in maximum 15 days from when the written request of the user has been received.

6. Your personal data rights

According to European Union applicable data protection legislation (GDPR), data subjects shall have the right to access to data, rectification, erasure, restriction of processing, objection to processing and right to data portability.

For any data processing based on consent, you have the right to withdraw the consent at any time.

For exercising these rights, you may send a written request, dated and signed to the above-mentioned flookyapps headquarters or via email to Data Protection Officer at privacy@flookyapps.com.

Data subjects are not subject to decisions based solely on automated processing, including profiling, which may produce legal effects or similarly significantly affects them.

You also have the right to lodge a complaint with a competent supervisory authority on data protection.

7. Additional information regarding personal data collection of certain flookyapps services and products

7.1. Anti-theft services of flookyapps products

This chapter complements the privacy policy with specific information regarding processing information which may be personal data and which is collected by flookyapps for the anti-theft services.

Part of the flookyapps products include the anti-theft service option designed for both mobile phones products as well as for tablets and laptops. Once activated and configured, the anti-theft option can track in real time via geo-localization the lost or stolen device. This flookyapps service offers the localization option as well as other connected options such as remote blocking of the device, deleting the entire content of the device or taking photos of the person who is accessing the phone without authorization. More details are available here.

In case the anti-theft services are activated, flookyapps may receive personal data such as geo-localization data either from GPS, GSM cells, Wi-Fi usage or IP address. The only purpose of processing these data is the functioning of the anti-theft service offered by flookyapps. For identifying the precise location, we may use third party services, as mentioned in Chapter 3.

All geo-localization information are kept for as long as the anti-theft service is active, but they will be deleted when the service is deactivated.

Anti-theft services may be remotely activated from your flookyapps system account (known as flookyapps Central). For this reason, it is highly important for your privacy and personal data protection not to reveal your password to unauthorized persons. For more advice in this regard, please see Chapter 3 of this document.

Thus, the owner of a flookyapps account may have administration rights for flookyapps services and products. Therefore, on the devices where the anti-theft services are installed, he/she can operate commands remotely. In this regard, the entire responsibility of the account owner is to ensure that he/she can fulfill these actions from a legal standpoint and that he/she has the right to know the location, to take pictures remotely, to block or delete

the device' content or to interact in any way with it. Therefore, we recommend activating the anti-theft service exclusively on your own devices or on devices where you have the right to legally do so.

7.2. Parental control services

This chapter complements the privacy policy with specific details regarding processing information which may be personal data and which are collected by flookyapps for the Parental Control services.

Some flookyapps products include a parental control option. If you buy such products or activate this option, you have the possibility to monitor your children's activity and to restrict access to certain, applications, websites or Internet services. This is only possible on supported devices (for example computers or phones) for which you have installed and activated flookyapps.

The parental control services option settings are managed from the web interface through which you access your flookyapps account (known as flookyapps Central). More details regarding the functionalities of this product are available on our dedicated webpage.

Before you can activate the parental control services, flookyapps will ask certain data for creating a profile – name, age and sex of the person. The name will be used exclusively for device identification purposes and you do not have to give your child's full name. Age and sex are necessary only for determining the default level of online protection offered by this product, which can be also later changed or configured by the account administrator.

Where this flookyapps parental control product is installed and an active profile is associated with the device, flookyapps may collect, exclusively for the purpose of providing parental control services, including for display in the parent’s account, detailed information about the use of the device such as: visited websites, search engine keywords, used applications and software, phone contacts, and geo-localization information.

The collected information depends on the settings configured by the parent in flookyapps Central. The only purpose of collecting this data is reporting to you, the parent. We do not use children information for their identification or monitoring Internet access by us.

We do not transmit to third parties the above-mentioned information for marketing purposes or any other information, which could lead to identifying your children.

When processing this data from your children's device, flookyapps acts as a technical intermediary. Therefore, the responsibility of a notice to your children regarding the installation of this software and the way the personal data is processed is exclusively up to you. You are the only one who may activate this option and specify which type of personal information you wish to be collected.

The flookyapps account owner has administration rights for flookyapps products and services, which includes parental control services. As such, he/she has full responsibility in assuring that he/she can undertake the surveillance activity from a legal point of view and

that he/she has the right to know the location, to block the content or applications from that device. Therefore, we recommend activating the parental control service exclusively on your minor children's devices or where you have the legal right to do so, based on the applicable law. We inform you that any illegal monitoring of online behavior or communications may be a crime. We do not recommend activating parental control services on devices used by persons who are over 16 years old, or otherwise in circumstances in which use of the parental control services is illegal.

7.3. VPN services

This chapter completes the rest of the privacy policy with specific details regarding processing information which may be personal data and which are collected by flookyapps through its VPN services.

Applying the data minimization principle, we collect for this service only randomly generated or hashed user and device IDs, IP addresses and randomly generated tokens to establish VPN connection for the sole purpose of providing the VPN service. For this service, we use Aura as data processor who processes data on behalf of flookyapps in accordance with flookyapps's instructions and for the sole purpose of providing VPN services to users.

We may process device location solely for the purpose of offering flookyapps VPN functionalities such notifications of unsafe Wi-Fi or the auto-connect feature. We do not store any details regarding your location or online activity nor do we share them with other entities.

7.4 Premium services

This chapter completes the rest of the privacy policy with specific details regarding processing information, which may be personal data that are collected by flookyapps for its Premium services.

As described and agreed by the Terms and Conditions for access to flookyapps Premium Services, these services cannot be performed unless we have access to your devices. Thus depending on the services selected, flookyapps may choose to provide the Premium Services using the following delivery channels: phone, live chat, email or remote access to your computer. During the delivery of the Services, flookyapps may, at its sole discretion and without any obligation, capture in different forms (such as, but not limited to: voice recording, video recording, screen recording, written recording, database monitoring) the Services sessions for the purposes mentioned below.

In order to ensure and avoid any liability issues on our interaction with your devices, we must record all interactions for providing the Premium Services between our staff and these devices. We do this specifically to protect you and/or flookyapps or its staff for any possible mismanagement in relation with your devices or your data. Please note that we may not provide the Services if you do not accept these recordings.

You will be properly informed whenever we start a recording and it will always stop when we disconnect from your devices.

The purposes of these specific data processing activities (recording the interactions between our staff and your devices) are to prevent liability issues from any contractual party for these services and to ensure services improvement, including quality assessments.

The legal basis for this processing is legitimate interest of our users and of flookyapps & its staff, based on Art 6 (1) f of GDPR. These data are being stored for a limited period – usually for maximum 12 month from the date of the communications, unless legal proceedings or liability issues are being raised on these communications in which case they will be stored until the end of such proceedings.

7.5 flookyapps BOX

This chapter completes the rest of the privacy policy with specific details regarding processing information, which may be personal data that are collected by flookyapps Box.

If you use flookyapps Box, the device will scan all the traffic in your network for malicious activity. This means that we will collect detailed technical data from all your smart devices that are connected to your network that will be used only for the purposes specified in Chapter 2.2. above.

In most cases, these technical data may not lead to your direct or indirect identification, but in some very specific cases, computer specialists might be able to identify a specific user. Therefore, we treat all such information as personal data and protect it as such.

If a new device from other users is connected to your network, flookyapps Box will also analyze network traffic from that device. It is your responsibility as network owner to inform the other users of your network that you use flookyapps BOX for the protection of the network traffic and therefore their traffic will also be analyzed, as described above.

7.6 flookyapps Digital Identity Protection

This chapter completes the rest of the privacy policy with specific details regarding processing information, which may be personal data that are collected by flookyapps Digital Identity Protection.

When you are using flookyapps Digital Identity Protection service, whether or not you are using only this service or along with a flookyapps anti-malware Solution, we ask you to provide us your name, e-mail address as well as non-mandatory additional information such as telephone number, home address, passport number, driver’s license number, gamer-tag, partial credit and/or debit card data, partial bank account number, partial Social Security Number and/or National ID number, partial insurance and/or medical insurance number for the purpose of providing you information security by:

providing you information related to breaches of your personal data and sending you instant alerts about any new breaches (you get instant alerts if your personal information shows up in a new data breach),

providing you the option of Continuous Identity monitoring in order to reduce false alarms or duplicated alerts we send you.

For any breach of your data, flookyapps Digital Identity Protection will alert you of the findings and you will be advised on the steps to take to reduce the risks of account take-over and new account fraud. Such findings may be references regarding e-mail, password, address, phone number, SSN, credit cards, travel documents, criminal records and medical records – without displaying the full value of such data unless such data has been provided by end user for data breach monitoring service, otherwise we are displaying only the reference that the data exists in the data breach and in certain instances partial (masked) data allowing the end user a hint for a better identification of their own data.

We provide you this service by using Constella Inc as data processor who processes data such as name, e-mail address and phone number on behalf of flookyapps in accordance with flookyapps's instructions and for the sole purpose of providing you flookyapps Digital Identity Protection services. The information that is provided to you via flookyapps Digital Identity Protection is collected as Data Controller by Constella Inc https://constellaintelligence.com/datalake-privacy-notice/ and as such, you can exercise your rights regarding this personal at privacy@constellaintelligence.com.

flookyapps Digital Identity Protection searches for personal information in publicly available sources to start mapping your digital footprint.

In order to provide you your digital footprint we may ask you to provide us your name, e-mail address and telephone number, for the purpose of providing you information security by:

providing you information regarding your digital footprint’s potential of damaging your online reputation or social media impersonation,

We provide you this feature by using PIPL as data processor who processes data such as name, e-mail address and phone number on behalf of flookyapps in accordance with flookyapps's instructions and for the sole purpose of providing you your digital footprint as part of flookyapps Digital Identity Protection service. The information that is provided to you via flookyapps Digital Identity Protection is collected as Data Controller by PIPL Inc https://pipl.com/.../privacy.../privacy-policy-individuals and as such, you can exercise your rights regarding this personal at https://pipl.com/customer-support.

We store the received information for as long as you have the service active in order to display to you the status of your information and to be able to properly notify or give you instant alert if a change regarding your Digital footprint has occurred or a data breach in which you are affected. Each time a new information appears, we will display it in the Digital Identity Protection section of your flookyapps Account.

7.7 flookyapps Password Manager

This chapter completes the rest of the privacy policy with specific details regarding processing information, which may be personal data that are collected by flookyapps Password Manager.

When you are using flookyapps Password Manager this service helps you remember credentials (usernames, passwords, PIN etc.) so that you can safely use strong unique passwords for every service you may access, as provided in the terms and conditions of this service or in the user's guide.

You will have full control all the time to your personal data in the Passwords vaults which may contain usernames, emails, passwords, secret keys, notes, addresses, personal IDs and credit card data. Vaults are not accessible to anyone, except the user; flookyapps does not have access or control of passwords. All passwords are encrypted with a key, that only the user of the service has knowledge about, in one single place (Password Manager), with complex master password requirements.

The user is able to use the features of flookyapps Password Manager after installation and sign-in in the browser extensions (Chrome, Firefox, Edge, Safari) and/or the mobile app (iOS and Android). The user will be prompted to use the account credentials stored in the Password Manager whenever they browse and land on the website that requires the log-in. Password Manager does not store nor transmits the Master Password or the security key, which means only the user has access to the user's vault.

7.8 flookyapps Identity Theft Protection

This chapter completes the rest of the privacy policy with specific details regarding processing information, which may be personal data that are collected by flookyapps Identity Theft Protection. Important note: this service is available only for US residents who have a SSN (social security number).

When you activate flookyapps Identity Theft Protection service we ask you to provide us your e-mail address for the purpose of providing you a functionality that provides ongoing monitoring, rapid alerts, and recovery services for protection against theft of your identity.

This functionality is included in the flookyapps Solution, a subscription based service, subjected to particular terms and conditions provided to you in the Subscription Agreement. We provide you this service by virtue of a third party software ("IdentityForce – a TransUnion brand") and it is licensed to you under the respective third party licenses mentioned herein: https://flookyapps.identityforce.com/terms-of-use. By accepting the Agreement for IdentityForce, You will have a direct relationship with Sontiq, a TransUnion brand and you will be informed about the collection and processing of personal data within their respective privacy policy: https://flookyapps.identityforce.com/privacy. Should you have any inquiries about Identity Theft Protection please email at flookyapps@identityforce.com or on other communication channels stated in their privacy policy.

flookyapps will transfer your e-mail address to Sontiq, a TransUnion brand, for the purpose of registration of the purchased service flookyapps Identity Theft Protection. Data is transferred on a one-off basis for the purposes of creating an account for IdentityForce, identity monitoring services such as dark web monitoring for the purpose of Identity Theft

Protection. This transfer of data is outside of EU for which flookyapps is Data Exporter as Data Controller and Sontiq, a TransUnion brand is Data Importer as Data Processor. If you contact the provider before the specific registration procedure for this service, they will handle your data (e-mail address, name and surname) as Data Processors for the following purposes: (1) the handling of phone calls with proactive inquiries, enrollment problems, or fraud issues; (2) monitoring of accounts of each user that enrolls and consents to the terms of use for the provision of services; and (3) any associated assistance and fraud remediation involving your personal data.

Once you register and accept IdentityForce terms of use and privacy policy, Sontiq, a TransUnion brand, will act as Data Controller and they may ask you to provide other personal data, including SSN which is necessary for fulfilling the registration for the services they provide according to their terms. IdentityForce may process financial data or government issued identification numbers. flookyapps however does not have access to financial data of the users nor to government identification numbers. IdentityForce is a software that includes monitoring the dark web for data sets provided directly by data subjects, including account numbers, government issued ID numbers, and other data. In particular cases it may include the management and remediation of fraud cases related to your identity by a service specialist based in Canada or the US.

Should you have any inquiries about your personal data please email them privacy@sontiq.com or on other communication channels stated in their privacy policy.

Personal data for this service is only retained for the duration it is needed by the user but no longer than one (1) year following the close of a case or cessation of monitoring.

8. Publication date

The privacy policy has been adopted on the date mentioned in the title of the document and will be modified each time is necessary without prior or future notice of the changes. The new version will enter into force when published on the website and it will be marked accordingly.