



## Privacy Policy (October 2020)

### Introduction

NEOS VENTURES LIMITED (“Neos”, “we”, “our”, “us”) respects your privacy and is committed to protecting and respecting your privacy and personal information in accordance with our obligations as controller under data protection law, including the European General Data Protection Regulation and Data Protection Act 2018 (“GDPR”).

This privacy policy will inform you as to how we look after your personal *information* when you purchase services from us, visit our website at <https://neos.co.uk/> (“website”) and download our Neos SmartHome application via Google Play at [https://play.google.com/store/apps/details?id=uk.co.neos.retail.android&hl=en\\_US](https://play.google.com/store/apps/details?id=uk.co.neos.retail.android&hl=en_US) or App Store at <https://apps.apple.com/gb/app/neos-smarthome/id1446759178> (“app”) and tell you about your privacy rights and how the law protects you.

### Website and app data processing

This privacy policy explains how we collect and process personal information in connection with an individual’s use of the app and the website and the services available therein for the purpose of supplying those services and contacting users and customers.

### Privacy policy format

This privacy policy is provided in a layered format so you can click through to the specific areas set out below. Alternatively, this policy will be available to you in your Neos app.

Please also use the Glossary to understand the meaning of some of the terms used in this privacy policy.

1. *IMPORTANT INFORMATION AND WHO WE ARE*
2. *DATA PROTECTION BY DESIGN AND DEFAULT*
3. *HOW IS YOUR PERSONAL INFORMATION COLLECTED?*
4. *THE PERSONAL INFORMATION WE COLLECT ABOUT YOU AND HOW WE USE IT*
5. *DISCLOSURES OF YOUR PERSONAL INFORMATION*
6. *WHERE WE STORE YOUR PERSONAL INFORMATION*
7. *INTERNATIONAL TRANSFERS*
8. *DATA RETENTION*
9. *YOUR LEGAL RIGHTS*
10. *GLOSSARY*

# 1. Important information and who we are

## Purpose of this privacy policy

This privacy policy aims to give you information on how Neos collects and processes your personal *information* through your use of the website, app and associated Smart Home devices, including any information you may provide by virtue of using our services when you contact, register with us and/or purchase a product or service.

It is important that you read this privacy policy together with any other policy we may provide on specific occasions when we are collecting or processing personal *information* about you so that you are fully aware of how and why we are using your data.

## Controller

Neos is the controller of personal *information* and responsible for your personal *information*. This means that Neos decides how your personal *information* is processed. Neos comprises the following business units:

- a. connected insurance: Administration of connected insurance which is underwritten by Aviva (Home Buildings & Contents) and ARAG (Home Emergency & Legal Expenses);
- b. connected products: sale of Smart Homes devices which is offered directly by Neos; and
- c. connected business: supply of connected products and services by Neos to Third Party Providers to their end customers which may be subject to further policies set out by the Third Party Provider.

## Neos and Aviva

Neos is an Aviva Group Company and may share certain personal information with other Aviva Group Companies as set out in the privacy policy.

## Data privacy manager and Information Commissioner's Office registration

We have resources for overseeing questions in relation to this privacy policy. If you have any questions about this privacy policy, including any requests to exercise your legal rights, please contact us using the details set out below.

## Contact details

If you have any questions about this privacy policy or our privacy practices, please contact our data privacy manager in the following ways:

Full name of legal entity:	Neos Ventures Limited
Email address:	hello@neos.co.uk
Postal address:	47 Bermondsey Street  London  SE1 3XT
Telephone number:	0203 210 3000

## Conflict resolution

You have the right to make a complaint at any time to the Information Commissioner's Office, the UK supervisory authority for data protection issues ([www.ico.org.uk](http://www.ico.org.uk)). We would, however, appreciate the chance to resolve any issues in the first instance.

## Changes to the privacy policy and your duty to inform us of changes

We keep our privacy policy under regular review. Historic versions can be obtained by contacting us. We may update this privacy policy from time to time. When we change our policy in a material way, we will update the version date registered on the document. For significant changes to this privacy policy we may give you a notice, however, please make sure you review this policy frequently to ensure that you are up to date with our processing activities.

It is important that the personal *information* we hold about you is accurate and current. Please keep us informed if your personal *information* changes during your relationship with us.

## Third-party links

This website may include links to third-party websites, plug-ins and applications. Clicking on those links or enabling those connections may allow third parties to collect or share data about you. We do not control these third-party websites and are not responsible for their privacy statements. When you leave our website, we encourage you to read the privacy policy of every website you visit.

## 2. Data protection by design and default

We are required by law to put in place appropriate technical and organisational measures to implement the data protection principles effectively, having regard to the nature of our business, and to safeguard individual rights. We endeavour to consider our data protection practices upfront in everything we do. It can help us to ensure that we comply with the GDPR's fundamental principles and requirements in our efforts to ensure transparency and accountability. Please see below how we comply with this obligation:

- We consider data protection issues as part of the design and implementation of systems, services, products and business practices.
- We make data protection an essential component of the core functionality of our processing systems and services.
- We anticipate risks and privacy-invasive events before they occur and take steps to prevent harm to individuals.
- We only process the personal *information* that we need for our purposes), and we only use the data for those purposes.
- We ensure that personal *information* is automatically protected in any IT system, service, product, and/or business practice, so that individuals should not have to take any specific action to protect their privacy.
- We provide the identity and contact information of those responsible for data protection both within our organisation and to individuals.
- We adopt a 'plain language' policy for any public documents so that individuals easily understand what we are doing with their personal *information*.
- We provide individuals with tools so they can determine how we are using their personal *information*, and whether our policies are being properly enforced.
- We offer strong privacy defaults, user-friendly options and controls, and respect user preferences.
- We only use data processors that provide sufficient guarantees of their technical and organisational measures for data protection by design.

### 3. How is your personal *information* collected?

Direct interactions	<p>You may give us your Identity, Contact and Financial Data (<i>please see clause 4 below for the specific types of personal information collected by Neos</i>) by filling in forms or by corresponding with us by post, phone, email or otherwise.</p> <p>This includes personal information you provide when you:</p> <ul style="list-style-type: none"> <li>• apply for and enquire about our products or services;</li> <li>• create a user account;</li> <li>• obtain and use services provided by us;</li> <li>• subscribe to our service or publications;</li> <li>• request marketing to be sent to you;</li> <li>• enter a survey; or give us feedback or contact us.</li> </ul>
---------------------	--

Third parties or publicly available sources	<p>We may obtain information about you from other sources. For example, we may collect information:</p> <ul style="list-style-type: none"> <li>• from publicly available sources;</li> <li>• when you interact with us on social media;</li> <li>• when you purchase one of our products or services through a third-party service; and</li> <li>• when you submit a review for one of products or services.</li> </ul> <p>This information includes information about:</p> <ul style="list-style-type: none"> <li>• your purchase of a Smart Home device or other service;</li> <li>• information from reviews you post;</li> <li>• username for third-party services;</li> <li>• social media profile information; and</li> <li>• demographic information.</li> </ul> <p>We may also obtain information about you from third-party sources, such as our partners or advertisers.</p>
Technical Data	<p>We may receive your Technical Data from the following sources:</p> <ul style="list-style-type: none"> <li>• directly from you;</li> <li>• analytics providers;</li> <li>• advertising networks; and search information providers</li> <li>• directly from you;</li> <li>• from the Third Party Providers in respect of the particular services provided to you; and</li> <li>• from Group or affiliated companies.</li> </ul>
Financial Data	<p>We may receive your Financial Data from the following sources:</p> <ul style="list-style-type: none"> <li>• directly from you;</li> <li>• from providers of technical, payment and delivery services; and</li> <li>• from the Third Party Providers in respect of the particular services provided to you; and</li> <li>• from Group or affiliated companies.</li> </ul>
Transaction Data	<p>We may receive your Transaction Data from the following sources:</p> <ul style="list-style-type: none"> <li>• directly from you;</li> <li>• from providers of technical, payment and delivery services; and</li> <li>• from the Third Party Providers in respect of the particular services provided to you; and</li> <li>• from Group or affiliated companies.</li> </ul>

#### 4. Personal *information* we collect about you and how we use it

Personal information means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

We will only use your personal *information* when the law allows us to. Most commonly, we will use your personal *information* in the following circumstances:

1. Where we need to perform the contract, we are about to enter into or have entered into, with you.
2. Where it is necessary for our legitimate interests (or those of a third party such as an Aviva Group Company or a Third Party Provider) and your interests and fundamental rights do not override those interests.
3. Where it is necessary to comply with a legal obligation, or to establish, exercise or defend legal claims.

Generally, we do not rely on consent as a legal basis for processing of your personal *information* although we will get your consent before sending third party direct marketing communications (marketing of services which are not specifically tailored to you) to you via email or text message and before we use your Geolocation Data. You have the right to withdraw consent at any time by contacting us.

Where we have indicated that we use our legitimate business interests, or the legitimate interests of a third party such as an Aviva Group Company or a Third Party Provider, we always document the nature of such interest and process personal *information* on the basis of such interests only in the circumstances where they are not infringing on data subjects' rights and freedoms. For the details concerning legitimate interests, please see the Glossary below.

We may collect, use, store and transfer different kinds of personal *information* about you which we have grouped together by as follows:

Type of data and description	General processing purposes	Purposes for processing via the app	Lawful basis for processing We constantly review the nature of our lawful bases for processing to ensure that each processing activity is on the basis of a specific, lawful and most appropriate basis for processing.
<b>Identity Data</b> Includes first name, maiden name, last name, username or similar identifier, marital status, title, date of birth and gender.	<ul style="list-style-type: none"> <li>• to provide our products and services to you;</li> <li>• to establish and manage your Neos account and profile;</li> <li>• to process and fulfil orders in connection with our products and services and keep you informed about the status of your order;</li> <li>• to identify and authenticate you so</li> </ul>	<ul style="list-style-type: none"> <li>• to install the app on your device;</li> <li>• to create your user profile;</li> <li>• to register your user profile;</li> <li>• to enable your access to our services;</li> <li>• to establish and manage your Neos account and profile;</li> <li>• to allow you to stream save and share content through the app;</li> </ul>	(a) Where it is necessary to perform a contract that we have entered into, or we will be entering into, with you, such as providing our products in accordance with the legal terms available at <a href="https://shop.neos.co.uk/pages/terms-conditions">shop.neos.co.uk/pages/terms-conditions</a> (b) Necessary for legitimate interests (please see the definition of the legitimate interests in the glossary below)

	<p>you may access certain content or use our services;</p> <ul style="list-style-type: none"> <li>• to increase and maintain the safety and security of our products and services and prevent misuse;</li> <li>• to allow you to interact with certain third-party products or services;</li> <li>• to protect against identify theft and prevent fraud and other criminal activity, claims and other liabilities;</li> <li>• to comply with and enforce applicable legal requirements, relevant industry standards and policies;</li> <li>• to recommend services which may interest you.</li> </ul>	<ul style="list-style-type: none"> <li>• to identify and authenticate you so you may access and use the app;</li> <li>• to increase and maintain the safety and security of our products and services and prevent misuse;</li> <li>• to check your identity;</li> <li>• to administer and protect our business and the app including troubleshooting, data analysis and system testing</li> </ul>	<p>(c) Necessary to comply with a legal obligation</p>
<p><b>Contact Data</b> Includes billing address, delivery address, email address and telephone numbers.</p>	<ul style="list-style-type: none"> <li>• to contact you in respect of our products and services that you are interested in;</li> <li>• to respond to your queries;</li> <li>• to bill you for the services;</li> <li>• to send you any information and updates relevant to the products and services which you have purchaser with Neos or otherwise interested in;</li> <li>• when you share comments and opinions with us, ask us questions or make a complaint we keep a record of this;</li> <li>• we may monitor and record our phone calls with you, in line with the legislation,</li> </ul>	<ul style="list-style-type: none"> <li>• Neos may process Contact and Identity Data such as name and description of your Neos product (for example, Neos SmartCam) and the location where you install your Neos product for the purposes of product setup and management;</li> <li>• we may send service messages directly to your mobile or smart device through the Neos app. Depending on the service you choose, you may also receive push notifications relating to the function of the Neos app, such as sensor alerts. You may also receive service message or notifications by text</li> </ul>	<p>(a) Consent (in respect of the location services) (b) Performance of a contract with you (c) Necessary to comply with a legal obligation (d) Necessary for legitimate interests</p>

	<p>to make sure we are living up to the standards we set;</p> <ul style="list-style-type: none"> <li>• we may process your Contact and Identity Data if you contact us through our “Contact Us” feature or customer support tools available on our website;</li> <li>• to communicate with you (including providing you with offers and other communications about our products and services) and provide customer support;</li> <li>• if you contact us through our “Contact Us” feature or customer support tools available on our website;</li> <li>• to allow you to interact with certain third-party products or services;</li> <li>• to comply with and enforce applicable legal requirements, relevant industry standards and policies.</li> </ul>	<p>message, phone or email depending on your products and service preferences. You can turn off service notifications at any time through your smartphone system settings.</p>	
<p><b>Financial Data</b> Includes bank account and payment card details.</p>	<ul style="list-style-type: none"> <li>• to collect payment for our services;</li> <li>• to allow you to interact with certain third-party products or services;</li> <li>• to perform analytics of anonymised personal information (including market and consumer research, trend analysis, financial analysis);</li> <li>• for the purpose of billing reconciliation, collection, auditing, accounting;</li> </ul>	<p>We may process your Financial and Identity Data if you choose to log in to your Neos account via Paypal, Facebook or any other third party, including when you share your Neos video and audio content via Facebook or any other social media site.</p>	<p>(a) Performance of a contract with you (b) Necessary for legitimate interests</p>



	<ul style="list-style-type: none"> <li>to protect against, identify theft and prevent fraud and other criminal activity, claims and other liabilities;</li> <li>to comply with and enforce applicable legal requirements, relevant industry standards and policies</li> </ul>		
<p><b>Transaction Data</b> Includes details about payments to and from you and other details of products and services you have purchased from us.</p>	<p>We may process your Transaction Data to personalise your experience with our products and services (including personalised marketing) and to manage and evaluate the effectiveness of our communications.</p>		<p>(a) Performance of a contract with you (b) Necessary for legitimate interests</p>
<p><b>Technical Data</b> Includes data and specifications relating to your internet protocol (IP) address, unique application number, your login data, browser type and version, time zone setting, browser plug-in types and versions, operating system and platform, and other technology on the devices you use to access the website and the app, details about the type of device, its operating system, the browser you use and applications on the device that connect to our products and services. It can also include details of your internet service provider, mobile network, current IP address and location.</p>	<p>We may process Technical Data to administer and protect our business, website and the app (including troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data).</p> <p>We may receive Technical Data from the following parties: (a) analytics providers; (a) search information providers.</p> <p>As you interact with the website, the app and your associated smart devices we will automatically collect Technical Data about your equipment, browsing actions and patterns. We collect this personal <i>information</i> by using cookies, server logs and other similar technologies. We may also receive Technical Data about you if you visit other websites</p>	<p>We may process Technical Data to administer and protect our business, website and the app (including troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data).</p> <p>We may receive Technical Data from the following parties: (a) analytics providers; (a) search information providers.</p> <p>As you interact with the website, the app and your associated smart devices we will automatically collect Technical Data about your equipment, browsing actions and patterns. We collect this personal <i>information</i> by using cookies, server logs and other similar technologies. We may also receive Technical Data about you if you visit other websites employing our cookies. Please see</p>	<p>(a) Performance of a contract with you (b) Necessary for legitimate interests</p>

	<p>employing our cookies. Please see our cookie policy on <a href="http://shop.neos.co.uk">shop.neos.co.uk</a> for further details.</p> <p>The app may process information relating to your Wi-Fi network, signal strength; and your Neos product model, serial number and software version.</p> <p>When you want to install or uninstall a service containing a unique device identifying number or when such a service searches for automatic updates, that number and information about your installation, for example, the type of operating system, may be sent to us (this is known as an application unique identifier).</p>	<p>our cookie policy <a href="http://shop.neos.co.uk">shop.neos.co.uk</a> for further details.</p> <p>The app may process information relating to your Wi-Fi network, signal strength; and your Neos product model, serial number and software version.</p> <p>When you want to install or uninstall a service containing a unique device identifying number or when such a service searches for automatic updates, that number and information about your installation, for example, the type of operating system, may be sent to us (this is known as an application unique identifier).</p>	
<p><b>Profile Data</b> Includes your username and password, purchases or orders made by you, your interests, preferences, feedback and survey responses.</p>	<p>Neos may process your Profile Data with respect to any records of any surveys you respond to or your entry into any competitions or promotions we may run from time to time.</p>	<ul style="list-style-type: none"> <li>• to enable you to use the services via the app;</li> <li>• to ensure security of your account;</li> <li>• to identify and authenticate you so you may access and use the app;</li> </ul>	<p>(a) Performance of a contract with you (b) Necessary for legitimate interests</p>
<p><b>Usage Data</b> Includes information about how you use our website and app, products and services.</p>	<p>We may process Usage Data to learn more about how our customers use our website, the app and your associated smart devices for the purpose of improving our website and our services.</p>	<p>We may process Usage Data to provide personalised services to our users and customers.</p>	<p>(a) Performance of a contract with you (b) Necessary for legitimate interests</p>
<p><b>Marketing and Communications Data</b> Includes your preferences in receiving marketing from us and our third</p>	<p>We may process Marketing and Communications Data to deliver relevant content and advertisements tailored to your interests.</p>	<p>We may process Marketing and Communications Data to understand the effectiveness of the advertising we serve to you.</p>	<p>(a) Performance of a contract with you (b) Your consent (in respect of direct marketing) (c) Necessary for legitimate interests</p>

parties and your communication preferences.		In accordance with the marketing preferences you set when creating your account or that you set up with us at a later date, we may contact you by email, push notification, text, mail or phone, to keep you updated on products and services.	
<b>Geolocation Data</b> Includes device geolocation data.	When using the auto-arming feature you are allowing Neos to use Android/Apple location services to determine if you (or any other member of the app) has left or returned from the defined geolocation set by the user. We can only operate these services when you have provided us with a defined location, enabled the auto-arming feature within the app and allowed location services to be enabled within your phone settings. We do not collect location data about your device when using this feature.	When using the auto-arming feature you are allowing Neos to use Android/Apple location services to determine if you (or any other member of the app) has left or returned from the defined geolocation set by the user. We can only operate these services when you have provided us with a defined location, enabled the auto-arming feature within the app and allowed location services to be enabled within your phone settings. We do not collect location data about your device when using this feature.	Your consent. You can withdraw your consent at any time by disabling Geolocation Data in your settings or contacting us.
<b>Aggregated Non-Personal Information<sup>1</sup></b> Could be derived from your personal <i>information</i> but is not considered personal <i>information</i> in law as this data	We may process your Aggregated Data to Operate, evaluate, develop, manage and improve our business (including operating, administering, analysing and improving our products and services;	We may process your Aggregated Data to Operate, evaluate, develop, manage and improve our business (including operating, administering, analysing and improving our products and services;	(a) Necessary for legitimate interests

<sup>1</sup> **Aggregated Non-Personal information** could also include communication, engagement and actions relating to our products and services, which are undertaken through external social media platforms, are subject to the terms and conditions as well as the privacy policies held with each social media platform respectively. Social media platforms should be used wisely and with due care and caution regarding your own privacy. Neos does not ask for personal or sensitive information through social media platforms and encourages you to contact us through primary communication channels such as by telephone or email. This website may use social sharing buttons which help share web content directly from web pages to the social media platform in question. You are advised before using such social sharing buttons that you do so at your own discretion and note that the social media platform may track and save your request to share a web page respectively through your social media platform account. However, if we combine or connect Aggregated Data with your personal information so that it can directly or indirectly identify you, we treat the combined data as personal information which will be used in accordance with this privacy policy.

<p>will <b>not</b> directly or indirectly reveal your identity. For example, we may aggregate your Usage Data to calculate the percentage of users accessing a specific website or app feature.</p>	<p>developing new products and services. <b>Analytics</b> We use third-party web analytics services on our websites and mobile app. The service providers that administer these services use automated technologies to collect data (such as email and IP addresses) to evaluate use of our websites and mobile apps to measure and analyse the effectiveness of the advertising we serve you and to monitor trends so we can improve the app.</p>	<p>developing new products and services. <b>Analytics</b> We use third-party web analytics services on our websites and mobile app. The service providers that administer these services use automated technologies to collect data (such as email and IP addresses) to evaluate use of our websites and mobile apps to measure and analyse the effectiveness of the advertising we serve you and to monitor trends so we can improve the app.</p>	
<p><b>Special Categories of Personal Information</b></p>	<p>Includes details about your race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions, trade union membership, information about your health, and genetic and biometric data).</p> <p>We do not knowingly collect any such data about you. However, as part of our services, Neos SmartCam may collect such personal <i>information</i> in the course of your use of our services, in which case we assure you that we do not intend to process such personal <i>information</i> for any purposes. Nor do we collect any information about criminal convictions and offences.</p>	<p>Includes details about your race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions, trade union membership, information about your health, and genetic and biometric data).</p> <p>We do not knowingly collect any such data about you. However, as part of our services, Neos SmartCam may collect such personal <i>information</i> in the course of your use of our services, in which case we assure you that we do not intend to process such personal <i>information</i> for any purposes. Nor do we collect any information about criminal convictions and offences.</p>	<p>Includes details about your race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions, trade union membership, information about your health, and genetic and biometric data).</p> <p>We do not knowingly collect any such data about you. However, as part of our services, Neos SmartCam may collect such personal <i>information</i> in the course of your use of our services, in which case we assure you that we do not intend to process such personal <i>information</i> for any purposes. Nor do we collect any information about criminal convictions and offences.</p>
<p><b>Aggregate Personal Information Collected via Neos SmartCam</b></p>	<p>Neos SmartCam is designed to allow you to see, hear and speak to anyone in within proximity of a given product from your</p>	<p>Neos SmartCam is designed to allow you to see, hear and speak to anyone in within proximity of a given product from your mobile</p>	<p>Performance of a contract with you</p>

	<p>mobile or smart device. To provide you with these services, we obtain aggregated content (and related information) that is captured and recorded when using Neos SmartCam, such as video or audio recordings, live video or audio streams, images, comments, and data our products collect from their surrounding environment to perform their functions (such as motion, events, temperature and ambient light). This information is processed to personalise your use of the Neos SmartCam.</p>	<p>or smart device. To provide you with these services, we obtain aggregated content (and related information) that is captured and recorded when using Neos SmartCam, such as video or audio recordings, live video or audio streams, images, comments, and data our products collect from their surrounding environment to perform their functions (such as motion, events, temperature and ambient light). This information is processed to personalise your use of the Neos SmartCam.</p>	
--	--	---	--

### If you fail to provide personal *information*

We may use the personal information we collect about you in other ways for which we provide specific notice prior to any such processing and will either obtain your consent to such processing or will provide a lawful basis upon which we seek to rely.

Where we need to collect personal information by law, or under the terms of a contract we have with you, and you fail to provide that data when requested, we may not be able to perform the contract we have or are trying to enter into with you (for example, to provide you with goods or services). In this case, we may have to cancel a product or service you have with us but we will notify you if this is the case at the time.

Prior to providing to Neos any personal information concerning another data subject (individual), you must (unless we agree otherwise): (a) inform the individual that you wish to share their personal *information* and refer them to this privacy policy; and (b) obtain their permission (where possible) to share their personal information with us in accordance with this Privacy Policy. Please ensure that you are not recording any personal *information* in a public space (even partially) where you do not have a lawful basis to record any such personal information. If you record any such data in the absence of a lawful basis under the GDPR, you shall notify us immediately. Capturing, recording or sharing video or audio content that involves other people may affect their privacy rights.

### Direct marketing

We may use your Identity, Contact, Technical, Usage and Profile Data to form a view on what we think you may want or need, or what may be of interest to you. This is how we decide which products, services and offers may be relevant for you (we call this direct

marketing). We will keep you up to date on news and exclusive offers from Neos, its partners and affiliated companies.

You will receive marketing communications from us if you have requested information from us or purchased services from us and you have not opted out from receiving direct marketing, or you have consented to receive such marketing. We strive to provide you with choices regarding certain personal *information* uses, particularly around direct marketing and advertising. You can let us know at any time that you do not wish to receive marketing messages by sending an email to us at [hello@neos.co.uk](mailto:hello@neos.co.uk) or contacting the customer service team via webchat. You are also able to turn off marketing permissions within the settings of your Neos app

However, while we are providing our services to you, we will continue sending certain specific communications relating to your Neos services. Such communications are necessary to enable us to provide the relevant services to you, therefore cannot be opted out from. Please refer to the table in paragraph 4 above to learn more about the lawful bases which we rely on to send such communications to you.

### Third-party marketing

We will get your express opt-in consent before we share your personal *information* with any third party for marketing purposes.

### Cookies

You can set your browser to refuse all or some browser cookies, or to alert you when websites set or access cookies. If you disable or refuse cookies, please note that some parts of the website may become inaccessible or not function properly. For more information about the cookies we use, please see our cookie policy [here](#).

### Change of purpose

We will only use your personal *information* for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If you wish to get an explanation as to how the processing for the new purpose is compatible with the original purpose, please contact us.

If we need to use your personal *information* for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal *information* without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law

## 5. Disclosures of your personal *information*

- Internal Third Parties.
- External Third Parties.
- Other third parties, including purchasers and prospective purchasers or other parties in any actual or proposed reorganisation, merger, sale, joint venture, assignment, divestiture, dissolution, liquidation, transfer or other transaction relating to all or any portion of our businesses, assets, companies or stock.

Alternatively, we may seek to acquire other businesses or merge with them. If a change happens to our business, then the new owners may use your personal information in the same way as set out in this privacy policy.

We require all third parties to respect the security of your personal information and to treat it in accordance with the law. We do not allow our third-party service providers to use your personal information for their own purposes and only permit them to process your personal information for specified purposes and in accordance with our instructions.

## 6. Where we store your personal *information*

We may use cloud storage providers to store your personal *information*. Each time we engage a new cloud service provider and consistently throughout our business relationship with such cloud service providers, we check that the security and availability of the service is right for the types of information we store. We endeavour to check that each cloud service provider has appropriate measures in place adopted to ensure safety of personal *information*.

Any payment transactions carried out by us or our chosen third-party provider of payment processing services will be encrypted. Where we have given you (or where you have chosen) a password that enables you to access to the app, you are responsible for keeping this password confidential. We ask you not to share a password with anyone.

We will collect and store personal *information* on your device using application data caches and browser web storage (including HTML5).

We may make available certain services including social networking, chat room or forum features via the app. When using these features, we will ensure that you do not submit any personal *information* that you do not want to be collected.

We have put in place appropriate security measures to prevent your personal *information* from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal *information* to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal *information* on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected personal *information* breach and will notify you and any applicable regulator when we are legally required to do so.

## 7. International transfers

Some personal information, for specific services, may be transferred to, processed or stored at locations outside of the UK or European Economic Area ("EEA") (including the USA), which have different data protection regimes to those in the EEA.

Any transfer of personal information which is undergoing processing or is intended for processing after transfer to a third country or to an international organisation will only take place in accordance with Chapter 5 of the GDPR and will only take place only if the

conditions laid down in the applicable section of Chapter 5 of the GDPR are complied with by us and each recipient, including for onward transfers of personal information from the third country or an international organisation to another third country or to another international organisation.

We will ensure that your data is treated securely and in accordance with this privacy policy and, when making these transfers, we will take steps to ensure that your personal information is adequately protected and transferred in accordance with the requirements of the GDPR. This typically involves the use of standard clauses in the form approved by the European Commission and permitted under Article 46 of the GDPR.

For further information about these transfers and to request details of the safeguards in place, please contact us using the details in paragraph 1 above.

## 8. Data retention

We will only retain your personal *information* for as long as reasonably necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, regulatory, tax, accounting or reporting requirements. We may retain your personal *information* for a longer period in the event of a complaint or if we reasonably believe there is a prospect of litigation in respect to our relationship with you.

After you close your account with us we will keep your personal information for a reasonable period to maintain our records and legal obligations to you.

Audio and video recordings will only be available to you, for the period specified in your service agreement.

To determine the appropriate retention period for personal *information*, we consider the amount, nature and sensitivity of the personal *information*, the potential risk of harm from unauthorised use or disclosure of your personal *information*, the purposes for which we process your personal *information* and whether we can achieve those purposes through other means, and the applicable legal, regulatory, tax, accounting or other requirements.

In some circumstances we will anonymise your personal *information* (so that it can no longer be associated with you) for research or statistical purposes, in which case we may use this information indefinitely without further notice to you.

In some circumstances you can ask us to delete your data: please see paragraph 10 (*Your legal rights*) below for further information.

## 9. Your legal rights

Under certain circumstances, you have rights under data protection laws in relation to your personal *information*. Please click on the links below to find out more about these rights:

- *Request access to your personal information.*
- *Request correction of your personal information.*
- *Request erasure of your personal information.*
- *Object to processing of your personal information.*
- *Request restriction of processing your personal information.*



- *Request transfer of your personal information.*
- *Right to withdraw consent.*

If you wish to exercise any of the rights set out above, please contact us using the contact details provided in paragraph 1 of this privacy policy.

### No fee usually required

You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. Alternatively, we could refuse to comply with your request in these circumstances.

### What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal information (or to exercise any of your other rights). This is a security measure to ensure that personal information is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

### Time limit to respond

We try to respond to all legitimate requests within one month. Occasionally it could take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

## 10. Glossary

### LAWFUL BASIS

Legitimate Interest means the our legitimate business interests, or the legitimate interests of a third party such as an Aviva Group Company or a Third Party Provider. We make sure we consider and balance any potential impact on you (both positive and negative) and your rights before we process your personal information on the basis of legitimate interests. We do not use your personal information for activities where such legitimate interests are overridden by the impact on you (unless we have your consent or are otherwise required or permitted to by law).

Where we rely on our legitimate interests or the legitimate interests of a third party (such as an Aviva Group Company or a Third Party Provider) to justify the processing of your personal information, our legitimate interests are:

- pursuit of our commercial activities and objectives, or those of a third party (for example, by carrying out direct marketing);
- improvement and development of our business operations, products and service offering, or those of a third party (for example by conducting research and analysis);
- provision of products and services which are tailored to your interests and to improve your experience;
- protection of our business, shareholders, employees and customers, or those of a third party (for example, ensuring IT network and information security, prevention of fraud, enforcing claims, including debt collection);

- seeking investment for, or in the context of, an actual or proposed reorganisation, merger, sale, joint venture, assignment, divestiture, dissolution, liquidation, transfer or other transaction relating to all or any portion of our businesses, assets, companies or stock; and
- analysing competition in the market for our services and to define types of customers for our products and services (for example, by carrying out research, including market research).

You can obtain further information about how we assess our legitimate interests against any potential impact on you in respect of specific activities by contacting us. Performance of Contract means processing your data where it is necessary for the performance of a contract to which you are a party or to take steps at your request before entering into such a contract.

Comply with a legal obligation means processing your personal *information* where it is necessary for compliance with a legal obligation that we are subject to.

## THIRD PARTIES

### Internal Third Parties

References to 'Aviva' are to one or more of the trading companies of Aviva that operate in the United Kingdom ("Aviva Group Companies"). For information about Aviva and for a list of Aviva Group Companies, see <https://www.aviva.co.uk>.

Neos is majority owned by an Aviva Group Company and may share personal data with Aviva Group Companies for the purposes set out in the table in paragraph 4 above where it is necessary for Neos' or an Aviva Group Company's legitimate interests. In most cases, Neos and any Aviva Group Company that receives personal data will each be data controllers. For more information about how Aviva processes personal data, see Aviva's privacy policy at <https://www.aviva.co.uk/services/about-our-business/products-and-services/privacy-policy/>.

### External Third Parties

- Service providers acting as processors who provide IT, cloud hosting, system administration and other services.
- Professional advisers acting as processors or joint controllers including lawyers, bankers, auditors and insurers who provide consultancy, banking, legal, insurance, accounting services, third parties involved in legal proceedings.
- HM Revenue & Customs, regulators and other authorities acting as processors or joint controllers based in the United Kingdom who require reporting of processing activities in certain circumstances.

### Third Party Provider

Those third parties with whom Neos has a commercial partnership.

## YOUR LEGAL RIGHTS

You have the right to:

**Request access** to your personal *information* (commonly known as a "data subject access request"). This enables you to receive a copy of the personal *information* we hold about you and to check that we are lawfully processing it.

**Request correction** of the personal *information* that we hold about you. This enables you to have any incomplete or inaccurate data we hold about you corrected, though we may need to verify the accuracy of the new data you provide to us.

**Request erasure** of your personal *information*. This enables you to ask us to delete or remove personal *information* where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal *information* where you have successfully exercised your right to object to processing (see below), where we may have processed your information unlawfully or where we are required to erase your personal *information* to comply with local law. Note, however, that we may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you, if applicable, at the time of your request.

**Object to processing** of your personal *information* where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground as you feel it impacts on your fundamental rights and freedoms. You also have the right to object where we are processing your personal *information* for direct marketing purposes. In some cases, we may demonstrate that we have compelling legitimate grounds to process your information which override your rights and freedoms.

**Request restriction of processing** of your personal *information*. This enables you to ask us to suspend the processing of your personal *information* in the following scenarios:

- If you want us to establish the data's accuracy.
- Where our use of the data is unlawful, but you do not want us to erase it.
- Where you need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal claims.
- You have objected to our use of your data, but we need to verify whether we have overriding legitimate grounds to use it.

**Request the transfer** of your personal *information* to you or to a third party. We will provide to you, or a third party you have chosen, your personal *information* in a structured, commonly used, machine-readable format. Note that this right only applies to automated information which you initially provided consent for us to use or where we used the information to perform a contract with you.

**Withdraw consent at any time** where we are relying on consent to process your personal *information*. However, this will not affect the lawfulness of any processing carried out before you withdraw your consent. If you withdraw your consent, we may not be able to provide certain products or services to you. We will advise you if this is the case at the time you withdraw your consent.

Customers who have their insurance underwritten by Aviva Insurance Limited (Aviva) will also be subject to the additional privacy policy in relation to their insurance policy with Aviva:

[Aviva Privacy Policy](#)

In this notice “we”, “us” or “our” means Aviva Insurance Limited.

Personal Information

Aviva collect and use personal information about you so that Aviva can provide you with a policy that suits your insurance needs. This notice explains the most important aspects of how Aviva use your data but you can get more detail about the terms Aviva use and view their full privacy policy at [www.aviva.co.uk/privacypolicy](http://www.aviva.co.uk/privacypolicy) or request a copy by writing to Aviva, Freepost, Mailing Exclusion Team, Unit 5, Wanlip Road Ind Est, Syston, Leicester LE7 1PD.

The data controller responsible for this personal information is Aviva Insurance Limited as the insurer of the product. Additional controllers include Neos Ventures Limited, who are responsible for the sale and distribution of the product, and any applicable insurers, reinsurers or brokers we use.

## Personal information Aviva collect, and it is used

Aviva will use personal information collected from you and obtained from other sources:

- to provide you with insurance: Aviva need this to decide if Aviva can offer insurance to you and if so on what terms and also to administer your policy, handle any claims and manage any renewal,
- to support legitimate interests that Aviva have as a business. Aviva need this to:
  - manage arrangements they have with insurers, reinsurers and brokers they use, and for the detection and prevention of fraud,
  - help Aviva better understand their customers and improve their customer engagement. This includes profiling and customer analytics which allows Aviva to make certain predictions and assumptions about your interests, make correlations about their customers to improve Aviva's products and to suggest other products which may be relevant or of interest to customers,
- to meet any applicable legal or regulatory obligations: Aviva need this to meet compliance requirements with their regulators (e.g. Financial Conduct Authority), to comply with law enforcement and to manage legal claims, and
- to carry out other activities that are in the public interest: for example, Aviva may need to use personal information to carry out anti-money laundering checks.

Aviva may also use personal information about other people, for example family members you wish to insure on a policy. If you are providing information about another person Aviva expect you to ensure that they know you are doing so. You might find it helpful to show them this privacy notice.

The personal information Aviva collect and use, will include name, address and date of birth, financial information and details of your home. If a claim is made Aviva will also collect personal information about the claim from you and any relevant third parties. Aviva may also need to ask for details relating to the health or any unspent offences or criminal convictions of you or somebody else covered under your policy. Aviva recognise that information about health and offences or criminal convictions is particularly sensitive information. Aviva will ensure that they only use that information where Aviva need to for our insurance purposes (including assessing the terms of your insurance contract, dealing with changes to your policy and/or dealing with claims).

There may be times when Aviva need consent to use personal information for a specific reason. If this happens Aviva will make this clear to you at the time. If you give Aviva consent to using personal information, you are free to withdraw this at

any time by contacting them – refer to the “Contacting Aviva” details below. Please note that if consent to use this information is withdrawn Aviva will not be able to continue to process the information you gave them for this/these purpose(s). This would not affect Aviva’s use of the information where consent is not required.

Of course, you don’t have to provide Aviva with any personal information, but if you don’t provide the information they need Aviva may not be able to proceed with your application or any claim you make.

Some of the information Aviva use as part of this application may be provided to Aviva by a third party. This may include information already held about you and your home within the Aviva group, including details from previous quotes and claims, information Aviva obtain from publicly available records, their trusted third parties and from industry databases, including fraud prevention agencies and databases.

## Credit Reference Agency Searches

To ensure Aviva have the necessary facts to assess your insurance risk, verify your identity, help prevent fraud and provide you with their best premium and payment options, Aviva may need to obtain information relating to you at quotation, renewal and in certain circumstances where policy amendments are requested. Aviva or their agents may undertake checks against publicly available information (such as electoral roll, county court judgments, bankruptcy orders or repossession(s)). Similar checks may be made when assessing claims.

The identity of our Credit Reference Agency and the ways in which they use and share personal information, are explained in more detail at [www.transunion.co.uk/crain](http://www.transunion.co.uk/crain)

## Automated decision making

Aviva carry out automated decision making to decide whether they can provide insurance to you and on what terms, deal with claims or carry out fraud checks. In particular Aviva use an automated underwriting engine to provide a quote for this product, using the information they have collected.

## How Aviva share your personal information with others

Aviva may share your personal information:

- with the Aviva group, their agents and third parties who provide services to Aviva, Neos Ventures Limited and other insurers (either directly or via those acting for the insurer such as loss adjusters or investigators) to help Aviva administer their products and services,
- with regulatory bodies and law enforcement bodies, including the police, e.g. if Aviva are required to do so to comply with a relevant legal or regulatory obligation,
- with other organisations including insurers, public bodies and the police (either directly or using shared databases) for fraud prevention and detection purposes,
- with reinsurers who provide reinsurance services to Aviva and for each other in respect of risks underwritten by Aviva, with insurers who cover Aviva under its group insurance policies and with their brokers who arrange and manage such

reinsurance and insurance arrangements. They will use your data to decide whether to provide reinsurance and insurance cover, arrange and manage such cover, assess and deal with reinsurance and insurance claims under such cover and to meet legal obligations. They will keep your data for the period necessary for these purposes and may need to disclose it to other companies within their group, their agents and third-party service providers, law enforcement and regulatory bodies.

Some of the organisations Aviva share information with may be located outside of the European Economic Area (“EEA”). Aviva will always take steps to ensure that any transfer of information outside of Europe is carefully managed to protect your privacy rights. For more information on this please see our Privacy Policy or contact Aviva.

### How long Aviva keep your personal information for

Aviva maintain a retention policy to ensure they only keep personal information for as long as they reasonably need it for the purposes explained in this notice. Aviva need to keep information for the period necessary to administer your insurance and deal with claims and queries on your policy. Aviva may also need to keep information after their relationship with you has ended, for example to ensure they have an accurate record in the event of any complaints or challenges, carry out relevant fraud checks, or where Aviva are required to do so for legal, regulatory or tax purposes.

### Your rights

You have various rights in relation to your personal information, including the right to request access to your personal information, correct any mistakes on our records, erase or restrict records where they are no longer required, object to use of personal information based on legitimate business interests, including profiling and marketing, ask not to be subject to automated decision making if the decision produces legal or other significant effects on you, and data portability. For more details in relation to your rights, including how to exercise them, please see our full privacy policy or contact Aviva – refer to the “Contacting Aviva” details below.

### Contacting Aviva

If you have any questions about how Aviva use personal information, or if you want to exercise your rights stated above, please contact their Data Protection team by either emailing them at [dataprt@aviva.com](mailto:dataprt@aviva.com) or writing to the Data Protection Officer, Level 5, Pitheavlis, Perth PH2 0NH.

If you have a complaint or concern about how Aviva use your personal information, please contact Aviva in the first instance and they will attempt to resolve the issue as soon as possible. You also have the right to lodge a complaint with the Information Commissioners Office at any time.