CONTINGENT WORKER DATA PRIVACY NOTICE

This privacy notice sets out important information about how your personal data will be processed when you apply for a contingent worker role with Aviva. Please ensure that you read this notice carefully and in full.

As a contingent worker engaged for an assignment with Aviva via a contract with a third-party vendor, when you share your information with us we use this information for a variety of purposes, including, but not limited to reviewing and assessing your engagement application and managing our ongoing relationship with you. This notice covers additional fair processing information for onboarding and managing for contingent working specifically. If you would like to know more about how and why we process your data within the context of an assignment, please read the *applicable People Privacy Notice for your jurisdiction*, as follows:

People Privacy Notice for your jurisdiction

UK People Privacy Notice

Ireland People Privacy Notice

We work with Randstad Sourceright (RSR), who provide us with services in relation to collecting information and administering your application on our behalf, as well as other contingent workforce and recruitment services.

As a contingent worker, you will enter into a contract with RSR or another third-party vendor, such as an employment agency. The third-party with whom you enter into a contract will process your personal data for their own purposes in accordance with its own privacy notice. For RSR, or other agencies' Privacy Notices, please contact the relevant agency who will be able to provide you with further information as to how your personal information is processed by them.

What Data will be Processed?

The categories of personal information about you that we may process are as follows:

- **Personal details**: given name(s); preferred name(s); nickname(s); former or maiden names; gender; date of birth / age; Social Security number, or local equivalent; passport number(s) other government issue number(s) including but not limited to tax identification number(s), driving license number(s), and immigration or visa related numbers; nationality; lifestyle and social circumstances; images of passports, and signatures; authentication data (passwords, challenge/response questions and answers, PINs; ID/security pass photographs.
- **Contact details**: address; telephone number; email address etc.
- **Screening Check Data**: ID documents (passport), proof of address, employment history, references, and, in some cases, criminal record checks, credit checks, fraud checks, media search, social media search, directorship check, biometric checks (via RSR's service provider Trust ID) or regulatory checks.
- **Workforce Activity**: Information you generate as a result of your work-related activities and content you create, such as documents, reports, or communications; records of time worked and not worked on assignment for the purposes of remuneration; system log on and off times, work location (in office vs. remote), hardware, systems and software use (including internet browsers), purpose and duration of use, calendar, email and other electronic communications metadata.

Processing Special Categories of Personal Data and Criminal Offence Data

In order to manage your application and assignments we may in some circumstances need to process Special Categories of Personal Data (such as health data) and/or Criminal Offence Data (subject always to local legal requirements), for example:

- compliance with a legal obligation (e.g., to comply with our health and safety obligations, or making reasonable adjustments);
- the detection or prevention of crime (including the prevention of fraud) to the extent permitted by applicable law;
- pre-assignment screening checks;
- you have manifestly made those sensitive Personal Data public;
- the establishment, exercise, or defense of legal rights;
- we have, in accordance with applicable law, obtained your explicit consent prior to processing your sensitive personal data (as above, this legal basis is only used in relation to processing that is entirely voluntary – it is not used for processing that is necessary or obligatory in any way); or
- reasons of substantial public interest, such as the promotion of equal opportunity and diversity, and is proportionate to the aim pursued and provides for suitable and specific measures to safeguard your fundamental rights and interests.

How and why will Your Data be Processed?

We collect personal data about you from a variety of sources (subject to local legal requirements) as follows:

- when you provide it to us (e.g., as a workforce applicant you provide personal information like your name, email address and telephone number so that we can contact you about possible employment opportunities).
- in the ordinary course of our relationship with you (e.g., in connection with your engagement).
- personal data that you choose to make public, including via social media (e.g., we may collect information from your social media profile(s) to the extent that you choose to make your profile publicly visible).
- personal data from third parties who provide it to us (e.g., recruitment agencies, credit reference agencies and law enforcement authorities).
- records of your interactions with us, and details of your engagement, subject to applicable law

Our Lawful Basis for Processing Your Personal Data

In addition to the purposes set out in the *applicable People Privacy Notice for your jurisdiction*, with regards to contingent worker onboarding and administration specifically we process for the following purposes:

Purpose/Activity	Lawful basis for processing including basis of legitimate interest

AML and Pre-Assignment Screening Checks: • fulfilling our own and assisting our clients and counterparties in meeting regulatory compliance obligations, including for engagement individual checks; confirming and verifying your identity (including by using credit reference agencies); screening against government, fraud prevention agencies (including Cifas) and/or law enforcement agency sanctions lists as well as internal sanctions lists and other legal restrictions. • to verify eligibility for an assignment, ensure safety and security, criminal records checks and to meet contractual or legal obligations. • We verify the information you provide (such as your qualifications, references and identity documents etc) to ensure it is accurate and to support our recruitment decision-making. We may use technology, including automated tools, to assist with checking the consistency and authenticity of this information	• compliance with a legal obligation; or • in connection with any contract that you may enter into with us, or to take steps prior to entering into a contract with us or the third party that enters into the contract for the assignment with you; • we have a legitimate interest in carrying out the processing for the purposes of preventing money laundering, sanctions violations and protecting against fraud (to the extent that such legitimate interest is not overridden by your interests or fundamental rights and freedoms); or • we have obtained your prior consent.
Application Administration: assessing your suitability for engagements.	• compliance with a legal obligation; or • we have a legitimate interest in carrying out the processing for the purposes of assessing your application for engagement (to the extent that such legitimate interest is not overridden by your interests or fundamental rights and freedoms); or • we have obtained your prior consent to the processing (this legal basis is only used in relation to processing that is entirely voluntary it is not used for processing that is necessary or obligatory in any way).
Contingent Workforce On-boarding and Offboarding: onboarding new Contingent Workforce; and compliance with our internal requirements, policies and procedures.	• compliance with a legal obligation; or • in connection with any contract that you may enter into with us, or to take steps prior to entering into a contract with us or the third party that enters into the contract for the assignment with you; • in connection with employment/worker law; • we have a legitimate interest in carrying out the processing for the purpose of on-boarding new Contingent; • when necessary to prevent fraud and ensure your safety in the identification and authentication process of registration in electronic systems; • we have obtained your prior consent.

Performance of Engagement Commitments	• compliance with a legal obligation; • in connection with any contract that you may enter into with us, or to take steps prior to entering into a contract with us or the third party that enters into the contract for the assignment with you; or • we have a legitimate interest in carrying out the processing for the purpose of fulfilling our engagement commitments, as required by contract, law and/or policy and procedure.
Administrative and Business Performance Reasons: including but not limited to time sheet and/or expense management; billing and invoicing as well as workforce analytics/metrics.	• compliance with a legal obligation; • in connection with any contract that you may enter into with us, or to take steps prior to entering into a contract with us or the third party that enters into the contract for the assignment with you; or • we have a legitimate interest in carrying out the processing for the purpose of fulfilling our engagement commitments, as required by contract, law and/or policy and procedure.

When we collect your personal data, we will inform you if it is required or voluntary. If the requested personal data is required, you will be informed of the potential consequences for failing to provide the data.

Sharing Data

We will process your data in accordance with as set out in the *applicable People Privacy Notice for your jurisdiction*.

Sharing with Cifas

Additionally, we will check your details against the Cifas databases established for the purpose of allowing organisations to record and share data on their fraud cases, other unlawful or dishonest conduct, malpractice, and other seriously improper conduct ('**Relevant Conduct**'). We and Cifas may also enable law enforcement agencies to access and use your personal data to detect, investigate, and prevent crime. Cifas will hold your personal data for up to six years if you are considered to pose a fraud or Relevant Conduct risk.

Should our investigations identify fraud or any other Relevant Conduct by you when applying for or during the course of your engagement with us, your new engagement may be refused or your existing engagement may be terminated or other disciplinary action taken (subject to your rights under your existing contract and under employment law generally). A record of any fraudulent or other Relevant Conduct by you will be retained by Cifas and may result in others refusing to employ you.

For further information see Cifas' Assessment of their Legitimate Interests in relation to the Insider Threat Database.

Transfers Oversees

We take steps to ensure that any transfer of personal data with our supply chain and/or outside the UK is carefully managed to protect your privacy rights and ensure that adequate safeguards are in place. Further details can be found in the *applicable People Privacy Notice for your jurisdiction*.

How long will we keep your data for?

We will hold your data in accordance with as set out in the *applicable People Privacy Notice for your jurisdiction*.

Protecting your Data

We are committed to protecting the confidentiality and security of your personal data as set out in the *applicable People Privacy Notice for your jurisdiction*.

Our supply chains are subject to contractual obligations to protect your personal data and process the data in accordance with our instructions. All individuals at Aviva that have access to your identifiable responses or are involved in creating reports/data analysis will be subject to strict confidentiality obligations in relation to access and use of the data and will have been given adequate training on how to handle the data confidentially.

Your Rights

You may have certain legal rights, depending on which country you are based in, in respect to your personal data. Subject to local data privacy laws, you may have a right to inquire about, access, rectify, erase, transfer and restrict or

object to our processing of your personal data. These rights are described in more detail in the “Your Legal Rights” section of the *applicable People Privacy Notice for your jurisdiction*.

If you are not happy with the way we or any of our third parties are handling your personal data, you can lodge a complaint with your local data protection regulator. However, we ask that you please attempt to resolve any issues directly with us first by contacting us via the details set out below.

Contacting Us

If you have any questions or concerns about how we use your personal data, please refer to the *applicable People Privacy Notice for your jurisdiction* for further details, including how to contact our Data Protection Officer.

If you have any other questions, please contact nonpermrecruitment@aviva.com