

Employee Privacy Notice



PartnerRe¹ (“**PartnerRe**”, “**we**” or “**us**”) is committed to protecting the privacy and security of your personal data.

This Employee Privacy Notice describes how and why we collect and use your personal data:

- i. when you apply to work or volunteer at PartnerRe
- ii. during your working relationship with us, and
- iii. after your working relationship with us.

It applies to all current and former employees, applicants, directors, interns, dependents, beneficiaries, contractors and temporary agency workers (“**you**” or “**your**”).

It is important that you read this Employee Privacy Notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal data about you, so that you are aware of how and why we are using such data.

Contents

1. APPLICATION OF LOCAL LAWS.....	2
2. WHAT DATA DO WE COLLECT ABOUT YOU (YOUR PERSONAL DATA)?	2
3. HOW IS YOUR PERSONAL DATA COLLECTED?	3
4. FOR WHAT PURPOSES DO WE USE YOUR PERSONAL DATA?	4
5. WHAT ARE THE LEGAL BASES ON WHICH WE USE YOUR PERSONAL DATA? ...	5
6. WITH WHOM DO WE SHARE YOUR PERSONAL DATA?	7
7. INTERNATIONAL TRANSFERS	7
8. RETENTION OF YOUR PERSONAL DATA.....	7
9. HOW DO WE PROTECT YOUR PERSONAL DATA?.....	8
10. AUTOMATED DECISION MAKING AND PROFILING.....	8
11. YOUR RIGHTS.....	8
12. YOUR RIGHT TO COMPLAIN TO THE SUPERVISORY AUTHORITY	9
13. IDENTITIES OF DATA CONTROLLERS – DATA PRIVACY OFFICER.....	9
14. CONTACT US	9
15. CHANGES TO THE EMPLOYEE PRIVACY NOTICE.....	9
16. GLOSSARY.....	9

¹ PartnerRe includes PartnerRe Ltd. and all direct and indirect subsidiaries and branches thereof



1. APPLICATION OF LOCAL LAWS

This Employee Privacy Notice is designed to provide compliance primarily with the EU GDPR, as well as the California Consumer Privacy Act.


Where relevant applicable local regulations require stricter standards than those described in this Employee Privacy Notice, we will ensure compliance with those stricter standards.

The rights and obligations contained in this Employee Privacy Notice may not be available to all individuals or in all jurisdictions. If you are unsure if or how this Employee Privacy Notice applies to you, please contact the Group Data Protection Officer (dataprotection@partnerre.com) for more information.

2. WHAT DATA DO WE COLLECT ABOUT YOU (YOUR PERSONAL DATA)?

Depending on the circumstances, we collect and process the following personal data about you (**where permitted by law**):

- ✓ **Personal details:**
 - About you: title, name, previous or maiden name, gender, nationality, civil/marital status, date of birth, age, personal contact details, national ID number, eligibility-to-work information, passport, ID, driving license, license plate number, utility bills, languages spoken; emergency contact information, details of any disability and any reasonable adjustments required as a result, physical and physiologic data (e.g. height, weight, eye color), national insurance number, national security number, photographs
 - About your dependents/relatives (first name, last name, date of birth)
- ✓ **Recruitment information:** skills and experience, qualifications, references, resume and application, interview and assessment data, background and verification information related to the outcome of your application, details of any offer made to you
- ✓ **Employment records:** contract of employment or engagement, work contact details, job titles, employee or payroll number, photograph, work location, working hours, days of work, worker ID and various system IDs, work biography, professional memberships, assigned business or support unit or group, reporting line, employee/contingent worker type, termination/contract end date, the reason for termination, last day of work, exit interviews
- ✓ **Regulatory information:** records of registration with any applicable regulatory authority, regulated status, including any criminal record or credit background checks which may be necessary, and any regulatory certificates and references, fitness and probity records
- ✓ **Remuneration and benefit information:** remuneration information (including salary/hourly plan/contract pay/fees information as applicable, allowances, overtime, bonus and commission plans), payments for leave, bank account details, grade, tax information, details of any benefits you receive or are eligible for, benefit coverage start date, expense claims and payments, information and agreements
- ✓ **Leave and absence management information:** attendance records, absence records, holiday dates, requests and approvals and information related to family leave or other special or statutory leave, absence history, fit notes, details of incapacity, details of work impact and adjustments, manager and Human Resources (HR) communications, return to work interviews
- ✓ **Performance management information:** colleagues and manager feedback, appraisals and performance review and rating information, outcome and objectives, performance improvement plans, talent program assessments and records, succession plans, formal and informal performance management process records

- 
- ✓ **Training and development information:** data relating to training and development needs or training received or assessment completed
 - ✓ **Disciplinary and grievance information**
 - ✓ **Employee claims, complaints and disclosures information:** subject matter of employment or contract-based litigation, complaints, disciplinary or grievance, pre claim conciliation, communications, settlement discussions, claim proceeding records, employee involvement in incident reporting and disclosures
 - ✓ **Images (Video, Photograph, Voice):** Images recorded by the closed circuit television system (CCTV); photo on access card; recordings of training, calls or meetings (such as the Group Video Conference, Airtime and other live events); images captured at company corporate and social events.
 - ✓ **Logging information:** information associated with your use of company resources such as download and print records, system and building login and access records, telepresence room reservations, information captured by IT security programs and filters.

Where permitted by law and necessary for a purpose, we also collect, store and use the following **special categories of personal data** which require a higher level of protection:

- ✓ Information about your health relevant to your work, including, for example, any medical condition, health and sickness records
- ✓ Information about criminal convictions and offences as part of a recruitment process
- ✓ Biometric data (e.g. fingerprints)
- ✓ Equality and diversity information: information regarding gender, age, nationality, religious belief, sexuality and ethnic origin.

Incidental collection of personal data:

PartnerRe IT Equipment² and your professional mailbox are corporate tools and are the property of PartnerRe. You must be mindful that if you use PartnerRe IT Equipment or your PartnerRe e-mail account to store or transmit folders, files, documents or any messages containing personal data, such folders, files, documents or messages and any attachment thereto could, to the extent permitted by applicable law, be accessed without prior notice to you (“Personal data incidentally collected”).


What if you do not provide personal data?

If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure your health and safety).

3. HOW IS YOUR PERSONAL DATA COLLECTED?

We collect your personal data from various sources, but mainly directly from you, when you apply to work or volunteer for PartnerRe and thereafter during your working relationship with us. You will usually provide this information directly to your managers or local Human Resources (HR) contact or enter it into our systems (for example, through your participation in HR processes, emails you send or through verbal information which will be recorded electronically or manually). In addition, we collect your personal data from your managers, HR, or occasionally your colleagues (for example, manager feedback and assessment, evidence from colleagues in investigations or peer review exercises).

² As defined in the PartnerRe Information Technology Guidelines



We also obtain some information from third parties: for example, references from a previous employer, medical reports from external professionals, information from tax authorities, benefit providers or where we employ a third party such as an employment agency, employment business or background check provider (**where permitted by applicable law**).

We also collect personal data which is publicly available on websites such as jobs boards, LinkedIn, or similar recruitment-related websites. We may use third-party applications which source their data from publicly available websites.

In some circumstances, your personal data will be collected indirectly (for example building and system access or use logs email and Internet records).

We collect additional personal data in the course of job-related activities throughout the period of you working for us.

4. FOR WHAT PURPOSES DO WE USE YOUR PERSONAL DATA?

We process your personal data for the following purposes. The list below also indicates, by numbers at the end of each category corresponding to the list in the section below “**WHAT ARE THE LEGAL BASES ON WHICH WE USE YOUR PERSONAL DATA?**”, the legal basis for which we may process **your personal data** (depending on the circumstances). Some of the bases for processing will overlap and there may be several grounds which justify our use of your personal data.

- ✓ Workforce planning, recruitment and staffing; [1, 4, 5, 6, 11]
- ✓ Workforce administration, payroll, compensation and benefit programs; [2, 3, 4]
- ✓ Performance management, learning and development; [4]
- ✓ Advancement and succession planning; [4]
- ✓ Working relationship termination; [2, 3, 4]
- ✓ Compliance with legal, regulatory, tax, health and safety obligations; [3, 7]
- ✓ Workforce compliance monitoring; [3, 4, 9, 12]
- ✓ Workplace management, such as travel and expense programs and internal health and safety programs; [4, 7, 8]
- ✓ Internal reporting; [4]
- ✓ Audit; [4]
- ✓ Data management in relation to Company-, Systems-, Processes- and Efficiency-developments; [4]
- ✓ Facility management; [4]
- ✓ IT equipment management; [4]
- ✓ Recording (such as Group Video Conference, training, webcast, team meetings) [4, 5, 6]
- ✓ Dealing with legal hold³, disputes, claims, including accidents at work [2, 3, 4, 10]
- ✓ Protection of PartnerRe, its workforce, and the public against injury, theft, legal liability, fraud or abuse or other injury; [4, 8] and
- ✓ Other business-related purposes (e.g. corporate communication, director or management appointments, organizing events, for books of business transfers, company sales & reorganisations). [4]

³ As explained in the Records Management Guidelines of PartnerRe



We also monitor and filter the use of company devices, our network, and internet traffic for lawful business purposes, and in particular for:

- ✓ Ensuring adequate information systems integrity and detecting and preventing criminal activity, including cyber-crime; [3, 4]
- ✓ Protecting information, including, but not limited to, personal data, confidential information, and high-value business information against destruction, loss, alteration, unauthorized access, disclosure or hacking; [3, 4]
- ✓ Securing the effective operation of its information systems; [4]
- ✓ Ensuring compliance with applicable regulatory and self-regulatory obligations; [3]
- ✓ Protecting the rights and property of PartnerRe, its staff, its counterparties; [4] and
- ✓ Detecting instances of non-compliance with PartnerRe’s policies and the Code of Business Conduct and Ethics. [3, 4]

Personal data incidentally collected through monitoring will not be used for purposes other than those for which the monitoring was introduced, unless it is clearly in your interest to do so or it reveals activity that PartnerRe could not be reasonably expected to ignore, for example an Employee suspected to be engaged in criminal activity.

Change of purpose

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

We may process your personal data without your knowledge or consent where this is **required or permitted by law**.

5. WHAT ARE THE LEGAL BASES ON WHICH WE USE YOUR PERSONAL DATA?

We are committed to processing your personal data fairly and lawfully and only to the extent necessary to achieve the purposes listed above.

We must have a legal basis to process your personal data. In most cases, our ability to obtain and process your personal data is based on one of the following legal bases:

Legal bases	Details
For processing personal data	
1. Pre contractual obligation ►	Processing is necessary in order to take steps at your request prior to entering into a contract
2. Performance of a contract ►	Processing is necessary for the performance of a contract to which you are a party
3. Compliance with a legal obligation ►	Processing is necessary for compliance with our legal obligation



4. For our legitimate interests ►	Processing is necessary for our legitimate interests as a data controller and employer and your interests and fundamental rights do not override those interests
5. Your explicit consent	<p>Where consent is required to process certain personal data, we will obtain consent from you (e.g. certain recordings).</p> <p>You are free to withdraw your consent at any time without affecting the lawfulness of processing based on consent before its withdrawal.</p>
For processing special categories of personal data	
6. Your explicit consent ►	<p>Where consent is legally required to process special categories of personal data, we will obtain consent from you.</p> <p>You are free to withdraw your consent at any time without affecting the lawfulness of processing based on consent before its withdrawal.</p>
7. Employment, social security and social protection law ►	Processing is necessary for the purposes of carrying out the obligations and exercising the rights of you or the Company in the field of employment law, social security and social protection law, to the extent permissible under applicable laws
8. Vital interests ►	Processing is necessary to protect your vital interests where you are physically or legally incapable of giving consent (for example in exceptional emergency situations, such as a medical emergency)
9. Assessment of the working capacity ►	Processing is necessary for the assessment of your working capacity (fitness to work)
10. Legal claims ►	Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.
11. Public data ►	Processing relates to personal data which you manifestly made public

12. Local law authorization ►

Processing is otherwise authorized by local law (e.g. monitoring equal opportunity).

6. WITH WHOM DO WE SHARE YOUR PERSONAL DATA?

Your personal data may be accessed by or disclosed to:

- Internally to other PartnerRe entities, PartnerRe employees;
- Joint ventures, subcontractors, processors, vendors or suppliers who perform services on our behalf for the aforementioned purposes;
- Existing or potential business partners
- The public for information made public on PartnerRe.com, depending on your function
- A newly formed or acquiring organization if PartnerRe is involved in a merger, sale or a transfer of some or all of its business;
- Any recipient, if we are required to do so, such as by applicable court order or law;
- Any recipient, such as for employment verification or bank loans; or
- Any recipient when reasonably necessary such as in the event of a life-threatening emergency.

7. INTERNATIONAL TRANSFERS

We transfer your personal data to recipients located in countries outside the European Economic Area (EEA). These countries' data protection laws may not offer the same level of protection for personal data as offered in the EEA.

Certain countries outside the EEA have been approved by the European Commission as providing essentially equivalent protections as EEA data protection laws. In such cases, EU data protection laws allow PartnerRe to freely transfer your personal data to such countries.

When we transfer your personal data to other countries outside the EEA, we establish legal grounds justifying such a transfer, mainly in the form of standard contractual clauses, or other legal grounds permitted by applicable legal requirements.

To regulate intra group personal data transfers, PartnerRe has executed a master data transfer agreement.

For more information on the appropriate safeguards in place, please contact us at the details contained in the **CONTACT US** section below.

8. RETENTION OF YOUR PERSONAL DATA

We will keep your personal data only for so long as is necessary to fulfil the purposes for which it was originally collected including for the purposes of satisfying any legal, accounting, or reporting requirements and any other permissible, related purpose. Beyond that, we retain personal data for a period of time that reasonably allows us to investigate, commence or defend legal claims brought by or against us, comply with our regulatory obligations and conduct analysis.

Once you are no longer an employee, an applicant, a director, an intern, a dependent, a beneficiary, a contractor or a temporary agency worker of PartnerRe, we will retain and securely destroy your personal data in accordance with applicable laws and regulations.



We may, instead of destroying or erasing your personal data, make it anonymous such that it cannot be associated with or tracked back to you.

As a general rule, we hold your data for the periods set out below:

Category	Retention
Employment records	1 up to 10 years after termination of contract
Employment applications	Up to 1 year after recruitment process finished

9. HOW DO WE PROTECT YOUR PERSONAL DATA?

We implement technical and organizational measures to ensure a level of security appropriate to the risk to the personal data we process. These measures are aimed at ensuring the on-going integrity and confidentiality of personal data. We evaluate these measures on a regular basis to ensure the security of the processing.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a data breach where we are legally required to do so.

Where we engage third parties to process personal data on our behalf, they do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organizational measures to ensure the security of data.


10. AUTOMATED DECISION MAKING AND PROFILING

Employment decisions are not based solely on automated processing.

11. YOUR RIGHTS

Under certain conditions, you have the right to ask us to:

- provide you with further details on the use we make of your personal data/special category of data (right to information);
- provide you with a copy of the personal data that you have provided to us (right to access);
- update any inaccuracies in the personal data we hold (right to rectification);
- delete any special category of data/personal data that we no longer have a lawful ground to use (right to erasure);
- in the rare cases where processing is based on your consent, stop that particular processing by withdrawing your consent (right to withdraw consent); withdrawal of your consent will not affect the lawfulness of processing based on consent before its withdrawal.
- object to any processing based on the legitimate interests ground unless our reasons for undertaking that processing outweigh any prejudice to your data protection rights (right to object to processing justified on legitimate interest grounds);
- receive your personal data in a usable electronic format and transmit it to a third party (right to data portability); and

- 
- restrict how we use your personal data whilst a complaint is being investigated (right to restriction of processing).

In certain circumstances, we may need to restrict the above rights in order to safeguard the public interest (e.g. the prevention or detection of crime) and our interests (e.g. the maintenance of legal privilege).

Your duty to inform us of changes

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

12. YOUR RIGHT TO COMPLAIN TO THE SUPERVISORY AUTHORITY

If you are not satisfied with our use of your personal data or our response to any request by you to exercise any of your rights in **YOUR RIGHTS** section, then you have the right to complain to your local supervisory authority (i.e. the supervisory authority in the jurisdiction where you live or work) or the supervisory authority of the jurisdiction where you believe an infringement of data protection laws has occurred. Each supervisory authority may have a different process for lodging complaints so we encourage you to contact the relevant supervisory authority first to check this.

13. IDENTITIES OF DATA CONTROLLERS – DATA PRIVACY OFFICER

To identify the PartnerRe entity responsible for the processing of your personal data, you can contact our Global Data Privacy Officer (dataprotection@partnerre.com).

14. CONTACT US

If you have questions or concerns regarding the way in which your personal data has been used, please e-mail our Data Protection Officer at dataprotection@partnerre.com.

15. CHANGES TO THE EMPLOYEE PRIVACY NOTICE

We may modify or update this Employee Privacy Notice from time to time,

Last updated: October 28, 2020.

16. GLOSSARY

GDPR is the EU **General Data Protection Regulation** (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC).

Personal data means any information relating to an identified or identifiable natural person; one who can be identified, directly or indirectly, by reference to an identifier such as name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special categories of personal data (also known as sensitive personal data) means personal data in the following categories: racial or ethnic origin, political opinions, religious or



philosophical beliefs, trade union membership, data concerning health or sex life or sexual orientation, genetic data, and biometric data where processed to uniquely identify a person.