SIRIUSPOINT INTERNATIONAL INSURANCE CORPORATION (SINT) and SIRIUS INTERNATIONAL MANAGING AGENCY (SIMA) JOB APPLICANT PRIVACY NOTICE

November 14, 2025

In connection with your application for a position within SiriusPoint you have been requested to provide us with your personal data, either directly to us or through a third-party recruitment agency that we have engaged for the recruitment of a specific position.

This notice describes how SiriusPoint, as a data controller, process personal information you provide to us in connection with your job application, and informs you about your rights and choices regarding access, correction and deletion of your personal data.

When you share your personal data with us through recruitment and assessment agencies, we will instruct our recruitment agencies to inform you of this privacy notice and how to get access to it. We will ask these agencies to only use your personal data in the context of the recruitment and selection services for us but we are not responsible for the processing activities that they undertake for their own purposes with your personal data. For these activities, we will ask you to check their privacy notices.

1 Definitions

"**Personal data**" is defined as any information relating to an identified or identifiable individual.

"**Sensitive Personal Data**" (also known as Special Categories of Personal data) includes for example personal data from which we can determine or infer an individual's racial or ethnic origin, political opinions, religious beliefs or other beliefs of a similar nature, membership of a trade union, physical or mental health or condition or sexual life.

"**Data controller**" Depending on the location of the position you have applied for, one of the following entities is the data controller with regard to your personal data, including personal data that we receive from recruitment agencies:

- **SiriusPoint International Insurance Corporation AB (publ)** (having its Head Office in Stockholm and branch offices in London, Liège and Zürich), or
- **Sirius International Managing Agency Ltd** (in London).

"**SiriusPoint**", "**we**" or "**us**" is referring to the relevant Data Controller as defined above.

2 What personal data do we process and how is it collected?

The personal data that we receive in connection with your application includes information

i. that you submit when applying for the position directly with us via our recruitment database Workbuster or via a recruitment firm,
ii. that we may collect from publicly available sources, such as your profile on LinkedIn,
iii. that you share during interviews and other communication with us or our recruitment agencies, and
iv. information collected and processed in the overall assessment/profile made by the recruitment agency, if such an agency is involved.

We may also collect personal data about you from former employers, such as references.

The categories of personal data that we process include:

- Name
- Sector of work and category
- Language skills
- Recruitment profile
- Contact details (such as e-mail address and telephone number)
- Years of working experience
- Notes from interview
- Results from personality and/or skill tests*
- Education
- Résumés
- Work permit details*
- Communication, such as e-mail, text messages and Inmail on LinkedIn
- Academic background
- Motivation letter (optional)
- Nationality
- Year of birth
- Your degrees
- Previous or current employers
- Background checks* (e.g. social media profiles, credit reports and references)
- Job preferences (e.g. willingness to travel)*

In places where there is an "*", this applies only when necessary for certain roles. As part of the hiring process we may, depending on the position you have applied for, perform personality and skill tests as well as background checks on you in order to further evaluate and validate your application. If background checks are performed, SiriusPoint will at all times ensure that applicable data privacy laws are complied with.

3 Why we process your personal data and the and legal basis for the processing of your personal data

In our recruitment process, we collect and use personal and sometimes sensitive personal data for a variety of reasons when processing your application for a job position with us. We may only process personal data about you if we have a valid lawful basis for doing so. Depending on the specific purpose for which we use your information we may rely on different lawful grounds for processing information about you. Please contact us

for more information about what lawful grounds we rely on for a specific processing operation where more than one lawful ground may apply as set forth in table below.

Where we rely on the legitimate interest ground for processing your personal data, we will balance the legitimate interest pursued by us and any relevant third party with your interest and fundamental rights and freedoms in relation to the protection of your personal data to ensure it is appropriate for us to rely on this particular lawful ground, and to identify any additional steps we need to take to achieve the correct balance of interest.

Purpose for processing	**Lawful basis for processing**
1. **To communicate** with you, SiriusPoint employees and third parties, to evaluate your eligibility for an open position (including informing you of future opportunities with SiriusPoint or its affiliates), and to take necessary steps at your request to initiate the recruitment process (messages, identification data and your contact details). 2. **To process and administering your job application** (including identification data, contact details, information about qualifications, employment history, information obtained during interviews, information contained in CV and Cover Letters). 3. **Determine eligibility** for the applied for position (including identification data, contact details, work and education experience, information from interviews, CV´s, Cover Letters information collected from relevant references that you have provided). 4. ***Background Checks** (including identification data, contacts details, information about qualifications and employment history, criminal records). 5. ** **Sensitive Personal Data** - only on case by case basis where relevant for determining eligibility.	Purposes for processing 1 to 4 • Legitimate interest of SiriusPoint; • Necessary for the performance of a contract with you; • Legal Obligations in relation to employment law; • Your explicit Consent. * Personal data relating to background checks will only be processed, when necessary, in order to fulfil legal obligations to which SiriusPoint is subject to. If no legal obligation applies, we will ask for your consent for such use of your personal data. ** We will ask for your consent as allowed by local data protection law in case we would need to process sensitive personal data. If such information is not specifically requested by us in the individual case, we ask that you do not submit any information which may qualify as sensitive personal data.

Processing Purposes and corresponding Lawful Basis for Sensitive Personal Data (where applicable).

Purpose for processing	Lawful basis for processing
1. To accommodate your application and for compliance with legal obligations.	• Your consent as allowed by local data protection law; and • Necessary to carry out the obligations and to exercise specific rights of the data controller or you regarding employment, social security and social protection law as permitted by local data protection law.
2. Criminal Records and background checks – where relevant and appropriate to the role you are applying for.	• Your consent as allowed by local data protection law; • Necessary to carry out the obligations and to exercise specific rights of the data controller or you regarding insurance, employment, social security and social protection law as permitted by local data protection law.

If you are hired at SiriusPoint as a result of your application, some of the personal data collected as part of the recruitment process may be transferred to your personnel file as necessary for the performance of the employment contract, as described in the relevant employee privacy notice. If you were not hired as a result of your application, we can, if you have agreed and given your consent, keep your personal data mentioned above (except notes from interviews and references) for up to one year to evaluate you for other positions which may become vacant within the mentioned time period.

4 Who has access to your personal data?

Access within SiriusPoint

Only persons who have a specific need to know within the context of their function within SiriusPoint will have access to your personal data. The following functions will be able to access your personal data:

- human resources functions;
- managers responsible for positions for the purposes of evaluation;
- in certain cases, IT-staff may also gain access to your data, but only to the extent necessary to ensure the proper functioning of our IT-systems and organization; and
- the local compliance / regulatory team depending on the nature of the role that has been applied for.

For certain positions we may share your personal data with other entities and branch offices within the SiriusPoint group located in the US, Canada and Bermuda to fulfil our legitimate interest to evaluate and administer your candidacy for SiriusPoint. Except for Canada, these countries are not considered by the EU, UK or Switzerland to provide adequate protection to personal data. Therefore, SiriusPoint has entered into the applicable Standard Contract Clauses with the receiving entities to ensure an adequate level of protection for personal data that is shared with them, unless other adequate safeguards are in place.

Data processors acting on behalf of SiriusPoint

When processing your personal data for any specific purposes detailed above, we may share your personal data with one or more third parties acting on behalf of SiriusPoint. **Data Processors** may carry out instructions and processing activities related to recruitment, training, administration, communication and other activities (for example companies that host, support and/or maintain the IT-systems or applications supporting our recruitment and other HR systems, e.g., "Workbuster").

All our Data Processors will be subject to contractual obligations to implement appropriate technical and organizational security measures to safeguard personal data, and to process personal information as instructed. Such security measures include, but not limited to, entering into appropriate Data Protection and Data Transfer Agreements, Standard Contractual Clauses, imposing restrictions on sub-processer to store and retain data within the EU/EEA, UK or Switzerland region wherever possible etc.

Other recipients

SiriusPoint may share your personal data with courts and outside counsels in case of a dispute in order to exercise, establish or defend legal claims to fulfill our and your legitimate interest to have disputes settled by competent courts. Your personal data may also be shared with courts and other authorities in order to fulfil our legal obligations.

5 International Transfers outside EU/EEA, UK or Switzerland

From time to time we may need to share your personal information with SiriusPoint affiliates that may be based outside of the EU/EEA, UK or Switzerland region. We may also allow our service providers, who may be located outside the EU/EEA, UK or Switzerland region, access or to process your personal information.

All international transfers to SiriusPoint affiliates and service providers will be protected by contractual commitments and where appropriate further assurances and supplementary measures, including standard contractual clauses adopted by the European Commission which gives specific contractual protections designed to ensure that your personal information receives an adequate and consistent level of protection.

Documentation of appropriate safeguards to countries outside the EU/EEA area

Upon request you are entitled to receive a copy of any documentation demonstrating that appropriate safeguards have been taken in order to protect your personal data during a transfer outside the EU/EEA, UK or Switzerland.

Information relating to the safeguards in place for all international transfers can be obtained by writing to designated DPO, please see below for contact details.

6 How long will your personal data be stored?

Your personal data will be retained as long as necessary to achieve the purpose for which it was collected, namely for evaluating your candidacy, plus any period as legally required or permitted by applicable law. This is normally the maximum statutory period in which a claim arising out of the recruitment process may be brought against us. After this time your information will be deleted, provided that no claim has been raised. Unsuccessful applications for positions in Germany are stored for maximum 4 months, unless actually required for litigation.

If you are hired at SiriusPoint as a result of your application some of the personal data collected as part of this recruitment process may be transferred to your personnel file and maintained for a longer period.

If you give your consent, we will maintain your personal data for a maximum period of one year or until you withdraw your consent, to evaluate and contact you for other positions which may become vacant within the mentioned time period.

7 What are your rights?

Under applicable data privacy laws (in some cases subject to certain conditions) you have the right to:

- Access and receive a copy of your personal data.
- Require us to rectify inadequate, incomplete or incorrect personal data.
- Object to certain processing of your personal data, when the processing is based on our legitimate interest.
- Request us to erase your personal data (including deleting or erasing your profile on Workbuster).
- Request us to restrict the processing of your personal data to only comprise storage.
- Withdraw your consent to a specific processing of your personal data, for example for the evaluation of you for other positions which may become vacant.
- Receive a machine-readable copy of personal data that you have provided to SiriusPoint or ask us transfer the data to another data controller (where possible).
- Lodge a complaint pertaining to our processing of your personal data with the relevant data protection authority.

8 Contact Information

If you have any questions or concerns regarding the processing of your personal data or wish to exercise any of your rights under applicable data privacy law or withdraw your consent to data processing, please contact SiriusPoint on the contact details set forth below. The data controllers for personal data are:

<u>Head office – Sweden</u>
Data Protection Officer

SiriusPoint International Insurance Corporation
Visiting address: Fleminggatan 14
SE-112 26 Stockholm
Sweden

Telephone: +46 (0)8 458 5500 (Switchboard)
E-mail: dpo@siriuspt.com

Local branch office – UK
Data Protection Officer
Sirius International Managing Agency Limited
Floor 3, 33 Gracechurch Street
London, EC3V 0BT
UK

Telephone: +44 (0)203 772 1000 (Switchboard)
E-mail: dpo@siriuspt.com

Local branch office – Belgium
Mont Saint-Martin
62 BE-4000 Liege, Belgium
+32 4 220 8611

Local branch office – Zürich
Dreikönigstrasse 12
CH-8002 Zurich, Switzerland
+41 43 443 01 80

9 Your right to complain to a 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 stated above, or if you think that we have breached the GDPR, then you have the right to complain to a local Data Protection supervisory authority, e.g. in the EU Member State of your habitual residence, place of work or place of the alleged infringement.

Below are contact details to the supervisory authorities in Sweden and the UK, where SINT has its main establishments.

UK - the Information Commissioners Office (ICO), http://www.ico.org.uk, telephone 0303 123 1113 or +44 1625 545 700 if you are calling from outside the UK.

Sweden – Integritetsskyddsmyndigheten (IMY), https://www.imy.se/, telephone +46(0) 657 61 00

Belgium – https://www.autoriteprotectiondonnees.be/

Switzerland – https://datenschutz.ch/