February 2023

DATA PROTECTION POLICY

Prescient Data Protection Mission Statement: *Going beyond compliance and building trust.*

This Data Protection Policy document supersedes all other policies relating to data protection. This document is applicable to all employees and representatives of the Prescient Healthcare Group companies (together, "Prescient").

Prescient is committed to compliance with international data protection laws. This Data Protection Policy applies worldwide to Prescient and is based on globally accepted principles on data protection. Ensuring data protection is the foundation of trustworthy business relationships and the reputation of Prescient as an attractive employer.

Principles for processing personal data

Personal data comprise any information that can directly or indirectly identify a natural person. Data protection laws govern how such data can be processed. The term "processing" is very broad. It essentially means anything that is done to or with personal data (including simply collecting, storing or deleting those data).

At Prescient, personal data will be:

a. Processed lawfully, fairly and in a transparent manner in relation to individuals;

b. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

c. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed, in accordance with Prescient's Data Retention Policy;

f. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures; and

g. Protected by appropriate safeguards when transferred outside of the United Kingdom and/or the European Union.

Lawful basis for processing personal data

To ensure its processing of data is lawful, fair and transparent, Prescient maintains a record of processing activities that is reviewed at least annually.

All data processed by Prescient must be done on one of the following lawful bases:

a. Consent in the form of a clear affirmative act that is freely given,

b. Fulfilment of a contract,

c. Legal obligation,

d. Vital interests,

e. Fulfilment of a public task, or

f. In pursuit of a legitimate interest.

Prescient will note the appropriate lawful basis relied upon in the record of processing activities. Where consent is relied upon as a lawful basis for processing data, evidence of consent will be kept with the personal data. Where communications are sent to individuals based on their consent, the option for individuals to revoke their consent should be clearly available and processes should be in place to ensure such revocation is reflected accurately in Prescient's systems.

Prescient classification

Depending on what or how personal data are being processed, Prescient may act as either a controller or a processor.

A 'controller' is a natural or legal person, public authority, agency or other body that, alone or jointly with others, determines the purposes and means of the processing of personal data. As an example, when conducting human-source elicitation (also referred to as 'primary competitive intelligence' research), our teams contact a wide variety of sources in the pharmaceutical industry to ask different questions. As we decide whom to contact and which questions to ask, and as we maintain our own records of these interactions, Prescient would be acting as a controller according to the GDPR's definitions and the UK Information Commissioner's Office's confirmation.

A 'processor' is a natural or legal person, public authority, agency or other body that processes personal data on behalf of a controller. As an example, Prescient would act as a processor if a client were to provide any personal data to us or if a client were to give us specific instructions to process personal data (e.g., "cover this particular KOL's presentation at this conference and tell us what the KOL said", "send us a list of speakers presenting about this class of drug", "conduct market research using these criteria").

Prescient must ensure contracts with clients, vendors and third parties comply with the standards set out by the Information Commissioner's Office (ICO) and, where applicable, include UK International Data Transfer Agreements (IDTAs) and EU Standard Contractual Clauses (SCCs). These contracts must include specific data protection clauses that clearly set out the data protection obligations, responsibilities and liabilities of each party, the subject matter and duration of the processing, the nature and stated purpose of the processing activities, the types of personal data to be processed, the categories of data subjects, and the obligations and rights of the controller.

All client, vendor and third-party contracts must be reviewed by Prescient's Data Protection Officer.

Registration with supervisory authorities

United Kingdom
Prescient maintains appropriate registrations with the UK's supervisory authority, the Information Commissioner's Office (ICO). Prescient's registrations can be viewed on the ICO's website at https://ico.org.uk/.

Germany
Prescient maintains an appropriate registration with the applicable German supervisory authority, the Hessian Commissioner for Data Protection and Freedom of Information.

Spain
Prescient maintains an appropriate registration with the applicable Spanish supervisory authority, the Spanish Data Protection Authority ("AEPD").

Data security

Personal data must be safeguarded from unauthorised access and unlawful processing or disclosure, as well as accidental loss, modification or destruction. This applies regardless of whether data are processed electronically or in paper form. Prescient has implemented an Information Security Policy, which all employees must follow.

Prescient will ensure that personal data are stored securely using state-of-the-art security measures and modern software that is kept up to date. Access to personal data shall be limited to personnel who need said access to perform their duties and appropriate security controls are in place to avoid unauthorised sharing of information. When personal data are no longer needed or when the retention period expires, personal data should be destroyed such that the data are irrecoverable. Employees should refer to the Information Security Policy for further details on these procedures.

To defend against cyber security attacks on Prescient's information assets, including individual user accounts, protective technical security measures have been implemented that monitor electronic communications to reduce security vulnerabilities and to preserve the confidentiality, integrity and availability of Prescient's electronic information assets.

Security incidents and data breaches

A 'security incident' is an event that compromises the confidentiality, integrity or availability of an information asset. A 'data breach' is a security incident that results in the confirmed disclosure – not just potential disclosure – of data to an unauthorised party and can require notification to the relevant supervisory authority and possibly the affected data subjects. All data breaches are security incidents but not all security incidents are data breaches.

Upon learning of a security incident leading to the accidental or unlawful destruction, loss, alteration, disclosure of, or access to personal data, Prescient employees should immediately inform Prescient's Data Protection Officer. Prescient will promptly assess the risk to people's rights and freedoms and, if appropriate, report this breach to the relevant supervisory authority and, if appropriate, the data subjects themselves. Prescient has implemented a Data Incident and Breach Policy that is to be followed in the event of a security incident or a breach of security.

Employees do not need to recognise the difference between an incident and a breach, but they do need to ensure that any type of event is reported promptly. Examples of incidents include a hard copy of a report being left in a public place, an email with personal data attached or embedded being sent to the wrong recipient, or an unauthorised third party gaining access to an employee's computer.

Client and partner data

Personal data of business prospects, clients and partners can be processed in order to establish, execute and terminate a contract. Prior to the execution of a contract, personal data can be processed to prepare bids, issue purchase orders or fulfil other requests that relate to contract conclusion. Prospects can be contacted during the contract preparation phase using the information that they have provided. Any restrictions requested by the prospects must be honoured.

Due to contractual obligations, Prescient often must process another entity's personal data as well as data on behalf of another entity. The principles listed above for processing personal data will be followed. If Prescient acts as a processor in processing another entity's (controller's) personal data, then it will do so only upon written instructions from the entity. Employees must save these instructions in the appropriate project folder.

Taking into account these instructions, any applicable agreements and relevant data protection laws, Project Managers are responsible for ensuring all data protection obligations are met for a given project.

Their responsibilities may include keeping an audit trail of where personal data are stored and how they are processed, obtaining written authorisation from the controller to use a subprocessor, and ensuring all relevant agreements are in place prior to the start of processing. A Project Manager will seek input and assistance where necessary from the Data Protection Officer.

Human-source elicitation

When conducting human-source elicitation on behalf of clients, all employees who perform this task are responsible for introducing themselves as calling from Prescient and, when appropriate, referring respondents to our privacy policy at www.prescienthg.com/privacy. Employees will use InflexionRx® or a Primary Intelligence Record in the corresponding project folder to keep notes when carrying out human-source elicitation. These notes must remain in the project folder or InflexionRx® at all times and must not be emailed, printed or saved in another location. Project Managers have the responsibility of monitoring that their teams follow this policy. When producing deliverables for clients, employees will include no more personal data than absolutely necessary.

Market research

All employees who engage in market research are responsible for ensuring data subjects are provided with an appropriate consent form to review and sign prior to participating in a market research interview.

The consent form must clearly provide the data subject with the following:

a. An explanation of the purposes of the research.

b. Confirmation that the research will comply with data protection law and with the British Healthcare Business Intelligence Association's Legal & Ethical Guidelines and the codes of conduct for market research as set out by the Association for the British Pharmaceutical Industry.

c. The ability to provide explicit consent to each of the specific purposes for the processing of their personal data and/or special categories of personal data.

d. Clear information regarding their data protection rights by providing the appropriate privacy notice (available at either www.prescienthg.com/privacy or https://www.strategicnorth.com/info/gdpr-privacy-notice-market-research-respondents/, depending on the legal entity delivering the engagement), and an explanation that they have the right to withdraw their consent at any time.

e. The requirement for Prescient to report any adverse events or product complaints pertaining to the research sponsor's products that are mentioned during a market research interview.

f. Confirmation that Prescient will not use the research as an attempt to sell anything or influence thinking.

g. Unless instructed otherwise by the client, notification that Prescient will reveal the sponsor of the research at the end of the interview.

Employees will use the corresponding project folder to store consent forms when carrying out market research interviews. These consent forms must always remain in the project folder and must not be emailed, printed or saved in another location. Project Managers have the responsibility of monitoring that their teams follow this policy.

Privacy notices

If a data subject contacts Prescient to request information (e.g., material about a service), data processing to meet this request is permitted. If personal data are collected from a Prescient website

data subjects must be informed of this in a privacy notice and cookies policy. These policies must be integrated so that they are easy to identify, directly accessible and consistently available for data subjects.

If personal data are obtained directly from data subjects, Prescient's privacy notice must be supplied at the time the personal data are obtained. If the personal data are not obtained directly from the data subject, our privacy notice must be provided within a reasonable period of having obtained the personal data, which means within one month. If the personal data are being used to communicate with the data subject, then our privacy notice must be supplied at the latest when the first communication takes place. If disclosure to another recipient is envisaged, our privacy notice must be supplied prior to the data being disclosed.

Prescient's privacy notice and cookies policy are publicly available on our websites at www.prescienthg.com/privacy and https://www.strategicnorth.com/info/gdpr-privacy-notice-general/ .

Employee personal data

In employment relationships, personal data can be processed as needed to initiate, carry out and terminate the employment agreement. When a potential employment relationship is being explored, applicants' personal data can be processed. If a candidate ceases to be considered for an opening, the candidate's data must be deleted in observance of the required retention period, unless the candidate has agreed for his or her data to remain on file for a future selection process. If it should be necessary during the application process to collect information on an applicant from a third party, the requirements of the corresponding national laws must be observed.

It is important that Prescient maintains accurate contact information in case a member of staff has an accident. Information is held in confidence and is only used when needed. Each employee is responsible for maintaining an up-to-date record of personal details, home address and next of kin within our HR system. This information should be requested when an employee starts work and should be updated by the employee when and as needed.

All efforts will be made to avoid emailing curricula vitae ("CVs")/resumés and instead store these documents on a secure platform that is accessible to the employees who need to view them. If employees receive CVs/resumés by email and do not have access to the platform for uploading, they must forward them to dataprotection@prescienthg.com with the subject line "CV for Recruitment Platform". Once a CV/resumé has been uploaded to the platform, the forwarding employee will permanently delete it from all email folders.

There must be a valid lawful basis to process personal data that relate to the employment relationship but was not originally part of the performance of the employment agreement. This can include a legal requirement, the consent of the employee or the legitimate interest of Prescient. The purposes of processing can be found in Prescient policies made available to all employees.

The legitimate interests that Prescient relies upon to process employee personal data include: setting the annual budget; signing and managing legal documents; complying with client agreement provisions; performing internal audits; producing reports; invoicing clients for work; providing team building activities; abiding by employee dietary restrictions; producing an online staff directory; obtaining external legal advice; sending out requests for market research work; measuring marketing and client satisfaction; resourcing; keeping sales records; booking travel for employees; holding human resources records and providing travel insurance to employees. Prescient also relies on legitimate interest as the basis for holding emergency contact information for its employees.

Special categories of personal data

Special categories of personal data can be processed only under certain conditions. Special personal data comprise data about racial and ethnic origin, political beliefs, religious or philosophical beliefs, union membership, and the health and sexual life of the data subject. Moreover, data that relate to a

crime can often be processed only under special requirements under national law. If there are plans to process special personal data in a new or different method or for a new purpose, the Data Protection Officer must be informed in advance so that any necessary assessments may be completed.

Prescient may process special categories of personal data as part of certain client research projects; to provide health insurance to employees and their dependents; for occupational health purposes; for diversity, equity and inclusion (DEI) transparency reporting; and to support the creation of affinity groups. Prescient must obtain data subjects' explicit consent to process special categories of personal data, unless exceptional circumstances apply. Any such explicit consent must clearly identify what special categories of personal data will be processed, why they are being processed and to whom they will be disclosed.

International data transfers

In the event that personal data are transmitted from the United Kingdom, EU/EEA or Switzerland to a third country, there must be an adequacy mechanism in place prior to the transfer. This does not apply if transmission is based on a legal obligation. The Prescient companies have signed IDTAs and SCCs in order to facilitate international personal data transfers between themselves. Another entity, however, must sometimes give its consent for these transfers to be made so employees should always check with the Data Protection Officer as to whether the necessary adequacy mechanisms and data protection agreements are in place.

Rights of the data subject

Every data subject has the following rights:

a. **Right to be informed.** Data subjects have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR.

b. **Right of access.** Data subjects have the right to access and receive a copy of their personal data and other supplementary information relating to themselves. If personal data are transmitted to third parties, information must be given about the identity of the recipient or the categories of recipients.

c. **Right to rectification.** Data subjects have the right to have inaccurate personal data rectified, or completed if they are incomplete.

d. **Right to erasure ('right to be forgotten').** Data subjects may request their data to be erased without undue delay if the processing of such data has no legal basis, or if the legal basis has ceased to apply, or if the purpose behind the data processing has lapsed or ceased to be applicable for other reasons. Existing retention periods and conflicting interests meriting protection must be observed.

e. **Right to restriction of processing.** Data subjects have the right to request the restriction or suppression of their personal data. This is not an absolute right and only applies in certain circumstances.

f. **Right to data portability.** Data subjects have the right to receive their personal data provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided.

g. **Right to object.** Data subjects have the right to object to the processing of their personal data in certain circumstances. Data subjects have an absolute right to stop their data being used for direct marketing. The right to object does not apply if a legal provision requires the data to be processed.

Responding to data subject requests is the sole responsibility of the Data Protection Officer. Prescient employees must immediately inform the Data Protection Officer of any requests from data subjects to exercise their rights.

Confidentiality of processing

Personal data are subject to data secrecy. Any unauthorised collection, processing or use of personal data by employees is prohibited. Employees may only have access to personal data as is appropriate for the type and scope of the task in question. This requires a careful breakdown and separation, as well as implementation, of roles and responsibilities.

Employees are forbidden to use the personal data to which they have access through their employment at Prescient for private or commercial purposes, to disclose these data to unauthorised persons, or to make these data available in any other way. HR must inform employees at the start of the employment relationship about the obligation to protect data secrecy. This obligation will remain in effect even after employment has ended.

Data Protection Impact Assessments

If a type of processing is likely to result in a high risk to the rights and freedoms of individuals, then Prescient must complete a Data Protection Impact Assessment (DPIA) prior to the start of processing.

The assessment of whether processing is likely to result in a high risk would take into account the nature, scope, context and purposes of processing. Prescient will consider both the likelihood and the severity of any potential harm to individuals. Risk implies a more than remote chance of some harm. High risk implies a higher threshold, either because the harm is more likely, or because the potential harm is more severe, or a combination of the two.

Three types of processing will automatically require Prescient to undertake a DPIA prior to the start of processing. These types are:

1. Systematic and extensive profiling with significant effects

2. Large-scale use of sensitive data

3. Systematic monitoring of a publicly accessible area on a large scale

If employees become aware that the company is planning to process personal data in a new way, they must contact the Data Protection Officer so the Data Protection Officer can determine whether a DPIA is necessary.

Responsibility

All business leaders are responsible for overseeing that their departments are processing personal data in accordance with this policy. If an area of the business contemplates a new purpose for processing personal data, then the business leader is responsible for requesting authorisation from the Data Protection Officer prior to its implementation. The leader should involve the Data Protection Officer at the initial stages of the planning, giving suitable time for any necessary assessments to be conducted, such as the completion of a Data Protection Impact Assessment. Before the introduction of new methods of data processing, particularly new IT systems, technical and organisational measures to protect personal data must be defined and implemented. The measures must be based on the state of the art, the risks of the processing and the need to protect the data.

When beginning their employment with Prescient, all employees will undergo data protection training. Employees will also receive annual training to ensure that they have relevant knowledge about data protection and how it relates to their responsibilities as Prescient employees. If appropriate, annual training will also include the British Healthcare Business Intelligence Association (BHBIA) Legal and

Ethical Guidelines certification. If employees ever feel that they require more guidance on data protection within their roles, they should contact the Data Protection Officer at dataprotection@prescienthg.com.

All employees must inform their Line Manager and the Data Protection Officer immediately about any violations of this Data Protection Policy or applicable data protection laws and regulations. Violations for which individual employees are responsible can lead to internal disciplinary measures (e.g., formal verbal or written warnings or possibly termination) and/or sanctions under employment law. More information about Prescient's disciplinary procedures is available in the employee handbook.

The Data Protection Officer is ultimately responsible for this policy, with oversight responsibility from the Board of Directors and management of Prescient.

Contact

Data subjects may contact the Data Protection Officer at any time to exercise their rights, raise concerns, ask questions, request information or make complaints relating to data protection or data security issues. Employees are encouraged to contact the Data Protection Officer if they are unsure of their responsibilities regarding the use of personal data in the course of their roles.

Contact details for the Data Protection Officer are as follows:

CP House, 97-107 Uxbridge Road
Ealing, London W5 5TL
United Kingdom
dataprotection@prescienthg.com

Document History

Version	Date	Comment	Owner
0.1	2018-07	First draft	Mackie Adoniadis
0.2	2018-08	Second draft	Mackie Adoniadis
0.3	2018-08	Final draft and sign-off	Courtney Carlson
1.0	2018-09	Release	Mackie Adoniadis
2.0	2018-12	Incorporation of personal details policy	Mackie Adoniadis
2.1	2020-06	Update of legitimate interests	Mackie Adoniadis
2.2	2022-05	Addition of DPIA section	Mackie Adoniadis
2.4	2022-11	Review and update to incorporate elements from Strategic North's data protection policy	Ross Fenwick
2.5	2022-11	Review	Rebecca Rosser
2.6	2023-01	Incorporation of further information related to special categories of personal data, UK IDTA and DSAR information, data security	Ross Fenwick
2.7	2023-01	Review	Courtney Carlson
2.8	2023-01	Update of Prescient classification, data security and special categories of personal data sections	Ross Fenwick
2.9	2023-02	Strategic North review	John Grime, Sarah Morton
3.0	2023-02	Final draft and sign-off	Courtney Carlson