GSK's Binding Corporate Rules
GSK Public Policy Statement
November 2022

Introduction

GSK's (**we, us, our**) human resources (**HR**) and research and development (**R&D**) activities involve the processing of "personal information" (see Glossary), including the transfer of that personal information internationally. We are committed to exercising high standards of integrity in dealing with personal information and have adopted Binding Corporate Rules (**BCRs**) to enable us to make international transfers of personal information, within our group of companies, in compliance with data protection laws of the European Union and the United Kingdom, in particular the General Data Protection Regulation (Regulation 2016/679) (**GDPR**) and its equivalent in the United Kingdom.

What are BCRs?

Our BCRs comprise a number of documents, including our Privacy Policy and Privacy Standard, an intra-group agreement between GSK companies, and this Public Policy Statement. They are supported by training and audits. This Public Policy Statement is designed to explain the BCRs and to ensure individuals (**you**), whose personal information we process in the context of our HR and R&D activities, are aware of their rights under the BCRs and how to exercise them.

A glossary of terms used in this document can be found at the end. If you require further information, contact our EU/UK Data Protection Officer here: EU.DPO@GSK.com.

The scope of our BCRs

As a result of the United Kingdom ceasing to be a member state of the EU, we have two sets of BCRs, our **EU BCRs** and our **UK BCRs**. All references in this statement to BCRs shall mean both our EU BCRs and our UK BCRs. All references in this statement to the GDPR shall, in respect of our UK BCRs, mean the equivalent UK data protection laws including the UK Data Protection Act 2018 and the GDPR as it forms part of UK law (known as UK GDPR).

The **EU BCRs** apply to your personal information collected in the context of our HR and R&D activities (as further described below), where it is transferred internationally:

- by a GSK company that is subject to EEA data protection laws, in the EEA countries identified below;
- to a country outside the European Economic Area (**EEA**), where the laws do not provide adequate protection for personal information.

EEA Countries where approval has been obtained: GSK has received approval for our BCRs in: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania (R&D only), Slovakia, Slovenia, Spain, Sweden and Switzerland.

The **UK BCRs** apply to your personal information collected in the context of our HR and R&D activities (as further described below), where it is transferred internationally:

- by a GSK company that is subject to UK data protection laws;
- to a country outside the UK, where the laws do not provide adequate protection for personal information.

Our HR activities: These include (i) managing the recruitment process which includes all screening, background and criminal record checks; (ii) managing our workforce which includes salary and benefits administration; managing health care, pensions, employee assistance, leave, insurance and savings plans; managing sickness, health and wellbeing, inclusion and diversity; managing employee relations, disciplinary matters and terminations; providing work related accommodations or health and insurance benefits; responding to queries or requests; and managing post-employment records and activities; (iii) maintaining business operations which includes allocating asset and resources, conducting strategic planning and project management, creating budgets and financial statements, keeping audit trails and maintaining records; (iv) analysing our workforce so that we can better use and allocate company assets and human resources; (v) managing the sale of assets, mergers, acquisitions and re-organizations; (vi) communicating with personnel, including in an emergency, and creating content, such as recordings, videos or pictures for internal communication and educational purposes; (vi) managing training, development, performance and talent management; (vii) managing GSK IT products, systems, networks and communication channels including to enable these to be used by personnel, including managing access rights and acceptable use, creating backups and gathering statistical data on their use; (viii) legal and compliance activities which include complying with legal, regulatory and other requirements such as employment, social security and occupational health laws and regulations, income tax and national insurance deductions; complying with record-keeping and reporting obligations; completing equal opportunity monitoring and

reporting; conducting audits and risk management; complying with government inspections; responding to legal process, pursuing legal rights and remedies defending litigation and managing any internal complaints or claims; complying with internal policies and procedures; and monitoring activities as permitted or required by local law; (ix) monitoring GSK IT resource usage and corporate investigations; (x) health, safety and security activities; and (xi) operating the Speak Up process to allow concerns to be raised or reported internally.

Our R&D activities: These include, interventional and non-interventional clinical studies that are solely or jointly initiated, managed or financed by us, and associated regulatory compliance such as, safety monitoring and adverse event reporting. The personal information processed comprises information relating to "External Researchers" and "Research Subjects" (see Glossary).

Out of scope: Our BCRs do not govern the processing and transfer of personal information by our commercial divisions (e.g. personal information relating to consumers, or individuals connected with suppliers to our commercial divisions). That information is protected according to different lawful mechanisms. Our EU BCRs do not cover transfers of personal information by GSK companies located outside the EEA, where they are not subject to EU data protection laws. Our UK BCRs do not cover transfers of personal information by GSK companies located outside the UK, where they are not subject to UK data protection laws.

GSK companies covered by the BCR: Our BCRs are binding on all our group companies that have signed the intra-group agreement mentioned above. These group companies shall provide details of audits in relation to personal information processed under these BCRs to relevant supervisory authorities on request, and permit supervisory authorities to audit them to demonstrate compliance with these BCRs.

For the EU BCRs: GlaxoSmithKline (Ireland) Limited, an Irish company, has overall responsibility for ensuring that other group companies around the world comply with the EU BCRs, including remedying breaches of the EU BCRs.
For the UK BCRs: GlaxoSmithKline plc, a UK company, has overall responsibility for ensuring that other group companies around the world comply with the UK BCRs, including remedying breaches of the UK BCRs.

Our Rules (as reflected in our Privacy Standard)

1. We process personal information fairly and lawfully

We will comply with applicable laws relating to processing personal information. In the event of a conflict between these BCRs and applicable laws, which is likely to have a substantial adverse effect, including any legally binding requests for the disclosure of personal information by a law enforcement authority or state security body, this shall be reported to (for EU BCRs) GlaxoSmithKline (Ireland) Limited, or (for UK BCRs) GlaxoSmithKline plc, and the competent supervisory authority. Where applicable law prohibits the relevant group company from making such a notification to the competent supervisory authority then we will use our best efforts to obtain a waiver of this prohibition.

In the event that these efforts are unsuccessful, the group company will provide to the competent supervisory authority, for each 12 month period, general information in respect of the requests it has received from such authorities, including the number of applications for disclosure, the type of data requested and, if possible, the identity of the body requesting it.

At no time will any group company provide personal information to government entities in any country indiscriminately, disproportionately or on a large scale in a manner that goes beyond what is necessary in a democratic society.

Reason for processing: We only process personal information where we have a legitimate business purpose for doing so and the processing is necessary for that purpose. All processing aligns with an appropriate legal basis under the GDPR.

Legal basis for processing: We rely on the following legal bases to process personal information. Processing must be necessary:

- for the performance of a contract to which you are a party or to take steps at your request prior to entering into a contract;
- to comply with our legal obligations;
- for performance by us of a task carried out in the public interest;

- to protect your vital interests; or
- for legitimate interests pursued by us or a third party, provided these interests are not overridden by your own interests, rights and freedoms.

Special category information: Given the nature of "special category information" (see Glossary), extra safeguards apply. We only process special category information where:

- it is necessary for us to comply with our legal obligations and exercise our legal rights under employment laws;
- it is necessary to protect your vital interests, where you are physically or legally incapable of giving consent;
- processing involves personal information which are manifestly made public by you;
- it is necessary for the establishment, exercise or defence of legal claims;
- it is necessary for reasons of substantial public interest; or
- for the purpose of preventive or occupational medicine, the assessment of the working capacity of one of our employees, medical diagnosis, the provision of health or social care or treatment or the management of health and social care systems and services, either under applicable laws or under a contract with a healthcare professional. Under these circumstances, the processing will be undertaken by a healthcare professional bound by an obligation of professional secrecy or by another person subject to an appropriate obligation of secrecy.

Where it is required by law or where we are unable to rely on one of the above grounds to process your personal information, we will seek your unambiguous consent. Where processing special category information we will only do so where such consent is explicitly provided. If you provide your consent, you are free to withdraw it at any time. If you would like to do so, please let us know by getting in touch with us as set out in our Privacy Notices which are available here.

2. We collect and retain the minimum amount of personal information necessary to pursue specific, explicit and legitimate business purposes

We collect the minimum amount of personal information necessary to pursue each specified, explicit and legitimate business purpose. We ensure personal information is adequate, relevant and limited to the purposes for which we collect and/or further process it. Where we become aware that any personal information is inaccurate, we take every reasonable step to erase or rectify it without delay. Whenever possible, we rely on "anonymised information" (see Glossary) rather than using personal information to achieve our aims. We ensure personal information is accurate and, where necessary, kept up-to-date.

We maintain a record of all processing activities that we carry out on your personal information, which we make available to supervisory authorities on request. This record contains the contact details of each GSK company processing personal information, the purposes of processing your personal information (i.e. why we use your personal information), the categories of individuals, the types of personal information, the categories of recipients with whom we share your personal information, transfers of your personal information internationally and the relevant legal tool we use for that purpose, and where possible the envisaged retention limits and a general description of the security measures applied to the processing activities.

Where our use of personal information is likely to result in a high risk to your rights and freedoms, prior to processing, we carry out an assessment of the impact of the processing on the protection of your personal information. We carry out these data protection impact assessments with support from the EU/UK Data Protection Officer in order to address any risks in the processing, and to identify security measures and other mechanisms to ensure the protection of your personal information.

We retain personal information only for as long as necessary for a legitimate business purpose. We then delete, destroy or anonymise the personal information.

3. We explain how personal information will be used and your rights

Transparency: We are transparent about our personal information processing activities. We ensure that information about our processing activities is provided to you, as required by applicable laws, normally at the time of collecting the personal information. For information about how GSK uses your personal information, please see our Privacy Notices which are available here. At a minimum, we provide or ensure the provision of the

following.

Information about GSK:

- the identity and the contact details of the GSK company that acts as the "data controller" (see Glossary) of your personal information and, where applicable, that data controller's representative;
- the contact details of our data protection officer (the EU/UK Data Protection Officer);

Information on how we use your personal information:

- how and why we are allowed under applicable laws to collect and use your personal information, including the purposes of the processing for which the personal information are intended;
- if we use your personal information for a legitimate business purpose, information about that legitimate interest;
- information about whom we share your personal information, including the recipients or categories of recipients, if any;
- in what instances we transfer your personal information outside of your home country (or outside the EEA, if you are in the EEA);
- if we rely on these BCRs, or another legal mechanism to transfer your personal information internationally (to a country or organisation that is not deemed adequate under applicable laws), information on these BCRs or legal mechanism, and how you can obtain a copy of the BCRs or other legal mechanism;
- how long we keep your personal information including the period for which the personal information will be stored, or if that is not possible, the criteria used to determine that period;

Information on your rights regarding your personal information:

- information on your rights, including the right to request access, rectification or erasure of your personal information, or to restrict or object to the processing of personal information, or the right to request GSK transfers your information to another organisation;
- how you can withdraw your consent to us processing your personal information at any time;
- your right to lodge a complaint with a supervisory authority;

Information on particular processing activities:

- whether it is necessary for us to use your personal information by law or to fulfil a contract with you, and the consequences for you if you do not provide use with that information;
- whether we make decisions about you using your personal information through automated processes without human involvement (known as "automated decision making") including to predict behaviour or evaluate characteristics of a person (known as "profiling");
- if we conduct automated decision making or profiling, information about our approach, the significance of this processing and the consequences of the processing for you as an individual; and
- where we intend to use your personal information for additional purposes (other than those communicated to you), information on that additional purposes.

Where we obtain your personal information from third parties rather than directly from you, we may (subject to applicable law) not provide the above information to you if this is impossible or involves disproportionate effort.

Individual rights management: We allow you to exercise rights under the GDPR, including the rights outlined below (which may be subject to certain restrictions based on your circumstances:

(i) **right to access your personal information** – specifically, the right to obtain from us confirmation as to whether or not your personal information is being processed, and, where that is the case, access to your personal information and the following information:

- the purposes of the processing;
- the categories of personal information concerned;
- the recipients or categories of recipient to whom your personal information have been or will be disclosed, in particular recipients in third countries or international organisations;
- where possible, the envisaged period for which your personal information will be stored, or, if not possible, the criteria used to determine that period;
- the existence of your right to request from us rectification or erasure of personal data or restriction of processing of personal data concerning you or to object to such processing;
- your right to lodge a complaint with a supervisory authority;

- where your personal data are not collected from you, any available information as to their source;
- the existence of automated decision-making, including profiling and at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for you;
- where your personal information is transferred to a third country or to an international organisation, you have the right to be informed of the appropriate safeguards.

We shall provide a copy of your personal information undergoing processing. For any further copies requested by you, or where a request is manifestly unfounded or excessive, in particular because of its repetitive nature, we may charge a reasonable fee based on administrative costs. Where you make such a request by electronic means, the information shall be provided to you in a commonly used electronic form. Your right to obtain a copy of your personal information shall not adversely affect the rights and freedoms of others.

(ii) **right to rectify (correct) your personal information** – specifically you have the right to obtain from us without undue delay the rectification of inaccurate personal information concerning you. Taking into account the purposes of the processing, you shall have the right to have incomplete personal information completed, including by means of providing a supplementary statement.

(iii) **right to erase your personal information –** specifically you have the right to obtain from us the erasure of personal information concerning you without undue delay and we shall have the obligation to erase personal data about you without undue delay where one of the following grounds applies:

- the personal information is no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- you withdraw the consent on which the processing is based and where there is no other legal ground for the processing;
- you object to the processing and there are no overriding legitimate grounds for the processing;
- your personal information has been unlawfully processed;
- your personal information has to be erased for compliance with a legal obligation in to which we are subject; and
- the personal information has been collected in relation to the offer of information society services.

Where we have made the personal data information and are obliged pursuant to erase the personal information, we, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform other data controllers which are processing the personal data that you have requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

The right to erasure shall not apply to the extent that processing is necessary:

- for exercising the right of freedom of expression and information;
- for compliance with a legal obligation which requires processing by law to which we are subject or for the performance of a task carried out in the public interest;
- for reasons of public interest in the area of public health;
- for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes; or for the establishment, exercise or defence of legal claims.

(iv) **right to restrict or object to processing of your personal information.** Specifically, you shall have the right to obtain from us the restriction of processing of your personal information where one of the following applies:

- the accuracy of the personal information is contested by you, for a period enabling us to verify the accuracy of the personal information;
- the processing is unlawful and you oppose the erasure of the personal information and request the restriction of their use instead;
- we no longer need the personal information for the purposes of the processing, but we are required by the data subject for the establishment, exercise or defence of legal claims;
- you have objected to processing pending the verification whether our legitimate grounds override yours.

Where processing has been restricted, such personal information shall, with the exception of storage, only be processed with your consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest under EU law or EEA

Member State Law (for EEA transfers), or under UK law (for UK transfers). Where you have obtained restriction of processing you shall be informed by us before the restriction of processing is lifted.

(v) **right to data portability -** to provide a copy of your personal information to you or a third party, specifically: you have the right to receive the personal information concerning you, which you have provided to us, in a structured, commonly used and machine-readable format and have the right to transmit those data to another data controller without hindrance from us, where:

- the processing is based on your consent; and
- the processing is carried out by automated means.

In exercising your right to data portability, you shall have the right to have the personal information transmitted directly from one controller to another, where technically feasible. This right referred shall not adversely affect the rights and freedoms of others.

(vi) **right for us not to make automated decisions about you.** Specifically, you have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning you or which similarly significantly affects you. This shall not apply if the decision:

- is necessary for entering into, or performance of, a contract between you subject and us;
- is authorised by law to which we are subject and which also lays down suitable measures to safeguard the your rights and freedoms and legitimate interests; or
- is based on your explicit consent.

We shall implement suitable measures to safeguard your rights and freedoms and legitimate interests, at least the right to obtain human intervention on our part and for you to express your point of view and to contest the decision.

(vii) **right to withdraw your consent**– to where you have previously provided consent to us for us to process your personal information.

(viii) **right to object to processing conducted on a legitimate interest.** Specifically, you have the right to object at any time to the processing of your personal information based on the legitimate interests of the data controller or a third party, or if the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller.

(ix) **right to object to, and opt-out of receiving marketing communications**. Specifically, you have the right to object at any time to the processing of you personal information for the purposes of marketing.

We also comply with applicable laws in those countries that provide you with other rights in respect of your personal information. We may restrict your right to access your personal information in order to protect others (e.g. another individual's right of privacy) or to meet our legal obligations.

Automated decision-making: We make limited use of automated decision making procedures when processing personal information. We will only use automated decision making if:

- it is necessary for entering into, or performance of, a contract between us and you;
- it is authorised under a specific EU or Member State law (in relation to EU BCRs) or under UK law (in relation to UK BCRs), and the safeguards required to be implemented by that law have been implemented; or
- you have given explicit consent.

If you would like to exercise any of your rights, please let us know by getting in touch with us as set out in our Privacy Notice. Where you opt to exercise any right, we will try to provide information on the action we have taken in response within one calendar month. Depending on the complexity of your request and the number of other requests we are dealing with, we may need a further two months to provide this information. We will let you know within one month of receiving your request if our response will be delayed.

4. We do not use personal information for further purposes incompatible with the purpose for which it was originally collected

Purpose limitation: We will only process personal information in a way which is compatible with the specified,

explicit and legitimate business purpose for which it was originally collected. We will notify you of any new purposes for processing your personal information.

5. We use appropriate security safeguards

Safeguarding your Privacy: We implement appropriate technical and organisational security measures to prevent accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information. These measures are appropriate to the risks associated with using personal information and incorporate state of the art technologies.

Incident and breach management: We will notify supervisory authorities of personal data breaches (see Glossary) without undue delay and in any event within 72 hours of becoming aware of them, unless those breaches are unlikely to result in a risk to your rights and freedoms. We will notify you of personal data breaches if such breach is likely to result in a high risk to your rights and freedoms, and (at our discretion) in certain other circumstances. We maintain a record of personal data breaches which includes facts about the personal data breach, its effects (if any) and the remedial action taken to resolve the breach. We will make these records available to competent supervisory authorities on request.

6. We carefully control disclosure of personal information to third parties

Third Party Privacy Management: We disclose personal information outside of our group of companies where required by law, in connection with legal proceedings, and in other limited and lawful circumstances. We may also transfer personal information outside of our group of companies to: (a) third-parties acting on our behalf, including suppliers; or (b) other independent third parties, such as research and commercial partners or regulatory agencies.

Where we rely upon any third parties to process personal information on our behalf, we put in place appropriate contractual, organisational and operational controls with them to ensure the confidentiality and security of your personal information. We require that those third parties agree to all provisions set out in article 28 of the GDPR. If we discover that a third party is processing personal information inconsistently with requirements imposed by us, or applicable laws, we will take all reasonable steps to ensure the deficiencies are addressed as quickly as possible.

Onward transfers to third parties: Where we transfer personal information internationally from the EEA or the UK to third parties located in countries where data protection laws of that country do not offer an adequate level of protection for personal information, we put in place standard contractual clauses with the recipient of that personal information. These are contractual protections that are in a prescribed form approved by the European Commission (for transfers from the EEA) or by the Secretary of State or ICO (for transfers from the UK), as applicable (details of which are available here: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en and https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/). You are entitled to receive a copy of these standard contractual clauses and can request them by email to EU.DPO@GSK.com. These standard contractual clauses require both GSK as the sender, and the third party as the recipient, of your personal information to agree to comply with stringent contractual requirements relating to the handling of your personal information to ensure it is appropriately protected. You, as the individual data subject, are able to make a claim under the relevant standard contractual clauses if GSK or the recipient is in breach of those requirements.

Ensuring an essentially equivalent level of protection: We may disclose personal information within our group of companies and to third parties which are located in countries outside the EEA and UK where the data protection laws are not deemed to provide an adequate level of protection by the European Commission (for EEA transfers) or the Secretary of State (for UK transfers). Prior to the disclosure of personal information to recipients located in these countries, we conduct a multi-stage assessment process to consider whether our contractual protections (including the BCRs and any standard contractual clauses for onward transfers) provide adequate safeguards to ensure an appropriate protection of personal information:

- We consider whether the laws and practices of the recipient country weaken existing data protection measures, including whether the recipients of personal information can comply with their obligations to protect the personal information. This involves assessing whether the laws and practices of the country

involve the recipient disclosing personal information to, or providing access to personal information by, public authorities to an extent that exceeds what is necessary and proportionate.

- If this assessment indicates a risk that the BCRs may not provide appropriate safeguards to personal information, we consider whether we can impose additional measures to the transfer of personal information to ensure an essentially equivalent level of protection. This may involve applying additional technical security measures.
- The EU/UK Data Protection Officer, along with GlaxoSmithKline (Ireland) Limited (for EEA transfers) and GlaxoSmithKline plc (for UK transfers), will be involved in this assessment.
- We will inform other GSK companies of the outcome of this assessment, and require GSK companies to apply these additional security measures for similar transfers.
- Where we consider that we are unable to identify appropriate additional security measures to provide an essentially equivalent level of protection to personal information, or where instructed by a competent supervisory authority, we will inform other GSK companies, and end or suspend the transfer of such personal information.

Regulatory Filings: Where required under applicable data protection laws in any EEA Member State or the UK, we notify or obtain approval from the relevant supervisory authority with regards to processing of personal information (including international transfers of personal information), and ensure that the notifications or submissions for approval are kept up to date in the event of any changes.

7. We operate a complaints procedure and respect your right to a remedy

Making a complaint to us: If you believe we may not have complied with the rules set out in our BCRs, you are free to raise concerns directly with us and to have your complaint assessed under our internal complaints resolution procedure. We encourage you to raise privacy complaints through our Speak Up line.

HR activities: For employees and other individuals whose information is processed in connection with HR activities, a privacy complaint could be registered with your line manager (in the case of GSK employees), a country compliance officer, a local HR or legal representative, or the regional equivalent of any of these, all of whom will report the privacy complaint to the complaint channel, which will forward the complaint to the business unit's compliance group and the Privacy Team. They will independently assess the appropriate course of action in response to your complaint.

R&D activities: For individuals whose personal information is processed in connection with R&D activities, if you are a "Research Subject" (see Glossary), you should contact the clinician or researcher who is conducting the study, who will forward the complaint to our Privacy Team. If you are an "External Researcher" (see Glossary), a privacy complaint could be registered with GSK's country compliance officer, legal representative, or the regional equivalent, all of whom will report the privacy complaint to the complaint channel within GSK. They will independently assess the appropriate course of action in response to your complaint.

Escalation: Regardless of where we receive data privacy complaints they will be escalated: (i) to a GSK Privacy Contact, whose contact details are published on our website here; or (ii) to GSK's EU/UK Data Protection Officer at EU.DPO@GSK.com. The EU/UK Data Protection Officer represents the final avenue within GSK for complaint resolution relating to our BCRs. We endeavour to resolve complaints expeditiously and, unless exceptional circumstances apply, GSK will contact you in writing within one month. That communication will either: (a) indicate our position with regards to the complaint and any action we have taken, or will take, in response to the complaint; or (b) state when you will be informed of our position, which will be no later than two months thereafter. You can contact our EU/UK Data Protection Officer directly if you wish.

Making a complaint to a supervisory authority or courts:
For EU BCRs: You may submit a complaint in relation to our EU BCRs to any of the following: (i) the competent supervisory authority in the EEA country where you have your habitual residence, place of work, or where the alleged breach took place; (ii) the Irish Data Protection Commissioner or Irish courts (as the location of GlaxoSmithKline (Ireland) Limited); (iii) the courts of the EEA country from which your personal information was transferred by us; or (iv) the courts in the EEA country where you have your habitual residence.
For UK BCRs: You may submit a complaint in relation to our UK BCRs to the UK Information Commissioner or any UK courts (as the location of GlaxoSmithKline plc).

Following our internal complaints procedure in no way prejudices your right to use any of these options.

You may be entitled to obtain redress and, in certain circumstances, compensation where we breach the BCRs. If you raise a complaint and can demonstrate that you have suffered material or non-material damage most likely because of a breach of either or both of our EU BCRs or UK BCRs, we will need to prove that there has been no breach of the relevant BCRs.

If an EEA supervisory authority or court of an EEA country makes an order against a GSK company outside of the EEA in relation to our EU BCRs, and the GSK company is unable or unwilling for whatever reason to pay the damages or comply with the order within any applicable grace period, then GlaxoSmithKline (Ireland) Limited will pay the damages awarded to you directly, or ensure that the relevant GSK company complies with the order.

If the UK Information Commissioner (or its successor or replacement) or the courts of the UK make an order against a GSK company outside of the UK in relation to our UK BCRs, and the GSK company is unable or unwilling for whatever reason to pay the damages or comply with the order within any applicable grace period, then GlaxoSmithKline plc will pay the damages awarded to you directly, or ensure that the relevant GSK company complies with the order.

Glossary

- "adequate protection" or "adequate level of protection" means a level of data protection in a country outside the EEA (for EEA transfers) or the UK (for UK transfers) that, under data protection laws, is considered to provide adequate protection for individuals' rights and freedoms for their personal information.
- "anonymised information" refers to personal information rendered anonymous in such a manner that an individual is not or no longer identified or identifiable.
- "Complementary Worker" is understood within GSK to mean any individual(s), excluding GSK employees, who provide services for or on behalf of GSK, including on or off-site contingent workers, professional consultants, temporary staff, vendors and service contractors.
- "data controller" means a natural or legal person that determines the purposes and means of processing personal information, either alone or jointly with others.
- "EU/UK Data Protection Officer" means the data protection officer, who monitors compliance with our BCRs and is responsible for monitoring compliance with EU and UK data protection law. The EU/UK Data Protection Officer can be contacted at EU.DPO@GSK.com.
- "External Researcher" refers to external physicians or other healthcare professionals who participate or may participate in R&D.
- "personal data breach" means any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information.
- "personal information" refers to information that relates to an identified or identifiable individual.
- "Research Subject" refers to candidates for, or individuals participating in research activities, or individuals taking our products or treatments whose personal information we process in the pharmacovigilance context. Research Subjects include participants that are both external and internal to GSK.
- "special category information" refers to a subset of personal information relating to an individual's race or ethnicity, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data processed for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

November 2022