GSK's Binding Corporate Rules

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; in particular the General Data Protection Regulation (Regulation 2016/679) (**GDPR**).

What are BCRs?

Our BCRs comprise a number of documents, including our Privacy Policy, Privacy Standard and Standard Operating Procedures, 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, whose personal information we process in the context of our HR and R&D activities (**you**), 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 detail, a copy of our BCRs can be obtained by contacting our EU Data Protection Officer here: EU.DPO@GSK.com .

The scope of our BCRs

The 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 or other EU data protection laws, in the EU countries identified below;
- to a country outside the European Economic Area (**EEA**), where the laws do not provide adequate protection for personal information.

EU 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, Switzerland and the UK .

Our HR activities: These include the administration and management of our workforce; recruitment and screening activities; entering into an employment relationship; salary and benefits administration; training, development and performance; managing disciplinary and grievance proceedings; communicating with employees and providing references; communicating with employees in an emergency; operating the Speak Up process to allow concerns to be raised or reported internally; maintaining business operations and ensuring employees can access systems and perform their role; screening and monitoring employee communications; complying with legal, regulatory and other requirements applicable to us, including those arising under tax, health and safety, anti-discrimination, data privacy, employment and immigration laws and regulations, record-keeping and reporting obligations, audit obligations and government inspections; and responding to legal process, pursuing legal rights and remedies, defending litigation and managing internal complaints or claims. The personal information processed comprises information relating to current, past or prospective GSK employees or "Complementary Workers" (see Glossary) as well as spouses and dependents, as applicable.

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. They do not cover transfers of personal information by GSK companies located outside the EEA, where they are not subject to UK or EU 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. GlaxoSmithKline plc, a UK company, has overall responsibility for ensuring that other group companies around the world comply with the BCRs, including remedying breaches of the 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, this shall be reported to the data protection authority.

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:

(i) 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;
(ii) to comply with our legal obligations;
(iii) for performance by us of a task carried out in the public interest;
(iv) to protect your vital interests; or
(v) for legitimate interests pursued by us or a third party, provided these interests are not overriden 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:

(i) it is necessary for us to comply with our legal obligations and exercise our legal rights under employment laws;
(ii) it is necessary to protect your vital interests, where you are physically or legally incapable of giving consent;
(iii) processing involves personal data which are manifestly made public by you;
(iv) it is necessary for the establishment, exercise or defence of legal claims;
(v) it is necesssary for reasons of substantial public interest; or
(vi) 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.

We seek your unamabiguous consent to process personal information and special category information where it is required by law, or where we are unable to rely on one of the above grounds.

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

We collect the minimum amount of personal information necessary to pursue each legitimate business purpose. We ensure personal information is adequate, relevant and not excessive in relation to the purposes for which we collect and/or further process it. 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 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 provide the information required by applicable laws, at the time of collecting the personal information. At a minimum, we provide the minimum information required under articles 13 and 14 of the GDPR. Where we obtain personal information from third parties rather than directly from you, we may (subject to applicable law) not provide this information to you if doing so would be impossible or involve a disproportionate effort.

Individual rights management: We allow you to exercise rights under the GDPR, including the right:

(i) to access your personal information;
(ii) to rectify your personal information;
(iii) to erase your personal information;
(iv) to restrict or stop processing of your personal information;
(v) to provide a copy of your personal information to you or a third party;
(vi) not to make automated decisions about you (see below);
(vii) to withdraw your consent; and
(viii) to opt-out of receiving marketing communications.

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).

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

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

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 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 data protection authorities of personal data breaches, 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 data protection 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 to third parties located in countries outside the EEA, where data protection laws do not offer an adequate level of protection for personal information, we implement approved standard contractual clauses (details of which are available *here* : https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en) exception for transferring the personal information.

Regulatory Filings: Where required under applicable data protection laws in any Member State, we notify or obtain approval from the relevant data protection 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 Centre of Excellence. 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 Centre of Excellence. 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, if they cannot be resolved they will be escalated: (i) to a GSK Country Privacy Advisor, whose contact details are published on our website

here; or (ii) to GSK's EU Data Protection Officer at EU.DPO@GSK.com. The EU 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 Data Protection Officer directly if you wish.

Making a complaint to a data protection authority or courts: You may submit a complaint to any of the following: (i) the competent data protection authority in the country where you have your main residence, place of work, or where the alleged breach took place; (ii) the UK Information Commissioner or UK courts (as the location of GlaxoSmithKline plc); (iii) the courts of the EEA country from which your personal information was transferred by us; and (iv) the courts in the EEA country where you have your main residence. Following our internal complaints procedure in no way prejudices your right to use any of these options.

If you raise a complaint and can demonstrate that you have suffered material or non-material damage most likely because of a breach of our BCRs, we will need to prove that there has been no breach of our BCRs. If a data protection authority or court makes an order against a GSK company outside of the EEA, 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

- "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.
- "External Researcher" refers to external physicians or other healthcare professionals who participate or may participate in R&D.
- "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.

June 2018