Safeguarding Personally Identifiable Information
A Summary of GSK's Binding Corporate Rules

The Issue

The processing of Personally Identifiable Information (PII)[1] and Sensitive Personally Identifiable Information (SPII)[2] is essential to GSK's Human Resources (HR) and Research & Development (R&D) functions, and involves the regular transfer of such information between GSK companies and between GSK and other companies.

GSK is committed to exercising high standards of integrity in dealing with PII,[3] and takes several measures to protect the PII of employees, researchers and clinical trial participants. For several years GSK has required all group companies, employees and suppliers to comply with its Global Privacy Policy. This reflects GSK's commitment to privacy and is designed to ensure that GSK adopts good privacy practices when conducting its business. The Global Privacy Policy is supported by more detailed Information Governance Standards (the Standards) on processing PII for HR and R&D activities.

GSK has now adopted Binding Corporate Rules (BCRs) to provide even more robust protection for PII that we process for HR and R&D activities. BCRs are essentially a legally binding company-wide global set of policies and rules based on European data protection laws that all GSK companies and employees must respect and that individuals have the right to enforce. In order to adopt BCRs we have updated our Global Privacy Policy, Standards and other key documents and procedures; created this summary document; and implemented an Intra-Group Agreement (IGA) that make the rules in all of these documents legally binding on all GSK companies.

This summary document is designed to explain the rules and help ensure that individuals who share their PII with GSK are aware of their rights under the BCRs and how to exercise those rights. GSK will post this summary of the BCRs on its internal and public websites and physical copies will be available from our Global Privacy Office upon request.

What are BCRs?

EU regulators developed the BCRs mechanism to allow multinational corporations, international organisations and groups of companies to make intra-organisational transfers of personal data across borders in compliance with EU data protection laws. BCRs permit companies to develop internal legally-binding commitments, based on EU law, on how they handle personal data irrespective of where this data is being processed. BCRs comprise various elements, including internal corporate guidelines, policies, training programmes and audits. BCRs also require companies to make it publicly known that individuals whose information they process have certain rights, and to advise individuals how they might go about enforcing those rights.

BCRs have to be approved by the Data Protection Authority (DPA) of each EU Member State in which the organisation will rely on the BCRs. The EU has developed a mutual recognition process that facilitates this approval process.

[1] **Personally Identifiable Information (PII)** refers to information, regardless of the medium in which such information is held or expressed, that identifies or that reasonably could be used to identify an individual.

[2] **Sensitive Personally Identifiable Information (SPII)** refers to a subset of PII relating to an individual's race or ethnicity, political opinions, religious or philosophical beliefs, trade union membership, commission of criminal offences (and related proceedings), health (including genetic data), sex life or sexual orientation, government issued identification numbers (e.g., social security numbers and national IDs), credit or debit card details or any other PII whose unauthorised acquisition, use, modification, loss or disclosure presents a greater risk of harm to the relevant individual.

[3] For the purposes of GSK's Standards and this document, unless otherwise specified, the term "PII" includes Sensitive PII.

The Scope of GSK's BCRs

GSK's BCRs apply to HR PII[4] and Research PII[5] that are collected in EEA Plus Countries[6] and are processed by GSK companies, wherever they are located, for HR and R&D activities:[7]

– HR activities refers to the administration and management of GSK's human resources, including recruitment and screening activities, salary and benefits administration, training and development, managing disciplinary and grievance proceedings and complying with legal and regulatory requirements applicable to GSK, including those arising under tax, health and safety, anti-discrimination, data privacy, employment and immigration laws and regulations.
– R&D activities include interventional and non-interventional clinical studies that are solely or jointly initiated, managed or financed by GSK and associated regulatory compliance such as safety monitoring and adverse event reporting.

GSK's BCRs are binding on all GSK companies that have signed the IGA. GSK plc has overall responsibility for ensuring that other GSK companies comply with the BCRs, including remedying breaches of the BCRs.

Our rules

1. We process PII fairly and lawfully

GSK will comply with applicable local laws relating to processing PII. Where there is no applicable local law or the law provides less protection than our BCRs, we will process PII in accordance with our BCRs. Where applicable local laws impose stricter requirements than arise under our BCRs, we will abide by the stricter requirements imposed by such laws. If any GSK company that has signed the IGA believes that applicable local laws prevent it from fulfilling its obligations under the BCRs and has a substantial negative effect on its compliance with the rules, it will promptly notify GSK plc unless it is prohibited to do so by a law enforcement or judicial authority.

PII: GSK only processes and transfers PII where unambiguous consent has been provided or where it is necessary for the performance of a contract to which the individual is party or to take steps at the request of the individual prior to entering into a contract; for GSK to comply with certain legal obligations; for public interest purposes; to protect the vital interests of the individual providing the PII; or for legitimate business purposes pursued by GSK or a third party - where such interests do not override the fundamental rights and freedoms of the individual providing the PII.

Sensitive PII: Given the sensitive nature of SPII, extra safeguards exist to justify and protect its use by GSK. These conditions include the need to seek explicit consent from the individual providing the SPII for the processing or only processing SPII where it is necessary for GSK to comply with its legal rights and obligations under employment laws; for the establishment, exercise or defence of legal claims; to protect the vital interests of the individual providing the PII or another person where the individual is physically or legally incapable of giving consent; or for key medical reasons related to the person who provided the SPII – 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. All these scenarios are clearly explained to individuals (see rule 3).

[4] **HR PII** refers to PII of current, past or prospective GSK employees or "Complementary Workers" as well as spouses and dependents, as applicable. ("Complementary Worker" is understood within GSK to mean any individual(s), excluding GSK employees, that provide services for or on behalf of the company, including on or off-site contingent workers, professional consultants, temporary staff, vendors and service contractors.)
[5] **Research PII** refers to PII of two sets of individuals: (i) external physicians or other healthcare professionals that participate or may participate in research and development (referred to within GSK as "External Researchers"); and (ii) candidates or individuals participating in research activities, or individuals taking GSK products or treatments whose personally identifiable information GSK processes in the pharmacovigilance context (referred to within GSK as "Research Subjects"). Research Subjects include participants that are both external and internal to GSK.
[6] **EEA Plus Country** refers to any country in the EEA (i.e., Member States of the European Union plus Norway, Iceland and Liechtenstein), as well as any country that the European Commission formally has determined provides adequate protection for PII as reflected in a published adequacy finding, including Argentina, Canada, Switzerland, Israel, New Zealand, Andorra, the Isle of Man, Guernsey, Jersey and the Faroe Islands.
[7] GSK's BCRs do not govern the processing and transfers of customer and supplier data by GSK's commercial divisions, which are protected using different lawful mechanisms.

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

GSK collects the minimum amount of PII necessary to pursue specific and legitimate business purposes as set out in the BCRs; this PII 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 rather than using PII to achieve our aims.

GSK maintains accurate and up-to-date records of the PII we process. We retain PII only for as long as necessary to fulfill legitimate business purposes and then archive, delete, destroy or anonymise the data as promptly and securely as possible.

3. We explain to individuals how their PII will be used and their rights regarding their PII

GSK provides individuals who share their PII with us information about how we plan to process their data, along with any other information required by applicable laws, at the time of collecting the PII. At a minimum, we will advise individuals of the following:

– our identity;
– the categories of PII that GSK processes;
– the legitimate business purposes for which GSK processes PII;
– their rights in and to the PII;
– the types of third parties with whom GSK shares PII; and
– the choices and means GSK offers individuals providing us with PII for limiting the use and disclosure of their information.

Where GSK obtains PII from third parties rather than directly from individuals, we may refrain (subject to applicable law) from providing this information if doing so would be impossible or involve a disproportionate effort.

GSK allows individuals resident in an EEA Plus Country access to, including receiving in a clear and understandable form, any PII relating to them held by GSK. They are in turn free to correct any incomplete or inaccurate PII and may also prevent the further processing of incomplete or inaccurate PII by GSK. Such individuals may also object on compelling, legitimate grounds to the processing of their PII, and GSK shall respect such requests wherever possible. For individuals resident outside of an EEA Plus Country, GSK complies with applicable laws in that country that provide individuals a right to access and correct their PII**.** GSK may restrict any individual's right to access their PII in order to protect the rights and freedoms of the individual or of others, including the rights and legitimate interests of GSK.

GSK makes limited use of automated decision making procedures when processing PII. More information about such procedures and controls that GSK puts in place to protect individuals in these circumstances is available upon request from the Global Privacy Office.

4. We do not use PII in a way that is incompatible with what has been explained to individuals

GSK may only process PII collected in an EEA Plus Country for a different or new purpose if GSK has a legitimate basis for doing so in accordance with the applicable law of the EEA Plus Country in which the PII was collected.

We have mechanisms in place to review and approve any "secondary" use of PII collected by HR or R&D functions for purposes unforeseen at the time of collection. These mechanisms for both HR and R&D PII do not apply if the relevant PII has been de-identified or aggregated (and thereby rendered anonymous), or if the secondary processing is required by law.

5. We use appropriate security safeguards

We adopt technical and organisational security measures to prevent accidental or unlawful destruction or accidental loss, alteration, disclosure of, or unauthorised access to, PII. These measures are appropriate to the risks associated with using PII and to the state of the art.

6. We carefully control disclosure of PII to third parties

GSK may be required to disclose PII outside of our company where required by law or legal process, to protect the interest of GSK and individuals, and in other limited and lawful circumstances. Further, as part of established business practice, GSK may need to transfer PII outside of our company or group of companies to:

- Third-party suppliers, i.e., agents working on GSK's behalf and under our direction, such as contract research organisations and local laboratories in the R&D context or payroll processors and benefits providers in the HR context; or
- Independent third parties such as research and commercial partners or regulatory agencies.

Where GSK relies upon any third parties to process PII for or on our behalf, we require them to put in place appropriate contractual, organisational and operational controls to ensure the confidentiality and security of the data.

Where GSK transfers PII collected in an EEA Plus Country to third parties located in a country considered by the EU to provide inadequate protection for PII, including to third parties in the U.S. who have not certified to the EU-U.S. Safe Harbor framework,[8] GSK implements a set of the European Commission's approved set of standard contractual clauses for such transfers, a set of clauses providing levels of protection commensurate with the standard contractual clauses, or relies on another lawful condition for transferring the data.[9]

If GSK discovers that a third party is processing PII inconsistently with our Standards or applicable laws, we take all reasonable steps to ensure the deficiencies are addressed as quickly as possible.

7. We have a Global Privacy Office and train our staff to ensure that we comply with the BCRs

The Global Privacy Office is run by our Global Privacy Officer, who reports directly and regularly to the Senior Vice President of Governance, Ethics and Assurance, who in turn reports to the Chief Executive Officer. The Global Privacy Officer leads the Global Privacy Team, which oversees data privacy compliance and sponsors several internal data privacy working groups who provide expertise on data privacy solutions and champion data privacy in business units and departments.

We support the implementation of every element of the BCRs through a robust awareness and training program, which is prepared and rolled out by the Global Privacy Office. At the heart of the privacy program is our internal website known as "Privacy is Personal", where GSK employees can globally access information about compliance tools and privacy initiatives underway at GSK. Privacy is Personal is the primary tool that the Global Privacy Office uses to raise awareness of privacy, and to educate and reinforce the privacy message to employees. In addition to this continually updated resource, the Global Privacy Office rolls out numerous communication campaigns at regular intervals to employees.

[8] A streamlined process that allows U.S. companies to certify that they comply with standards of privacy protection that satisfy EU rules regulating the transfer of data to third countries.

[9] Where the transfer is to a third-party supplier, GSK implements the standard contractual clauses for transfers of PII to non-EU data processors or a set of clauses providing levels of protection commensurate with the standard contractual clauses. Where the transfer is to an independent third party, GSK implements the standard contractual clauses for transfers of PII to non-EU data controllers, a set of clauses providing levels of protection commensurate with the standard contractual clauses, or alternatively, ensures that the transfer (i) takes place with the unambiguous consent of the individual, (ii) is necessary to conclude or perform a contract concluded with the individual, (iii) is necessary or legally required on important public interest grounds, or (iv) is necessary to protect the vital interests of the individual.

GSK also provides computer-based training modules on data privacy and specifically in relation to our detailed Standards. These modules contain periodic knowledge checks and are mandatory training for all GSK managers and above globally. GSK also enrols groups of employees within GSK who may not be managers, but who process PII in the course of their work activities.

8. We operate a complaints procedure and respect individuals' right to remedy

Individuals resident in an EEA Plus Country whose PII are processed by GSK and who believe we may not have complied with rules 1-6, 8 and 10 of our BCRs are free to raise their concerns directly with us and to have their complaint assessed under GSK's internal complaints resolution procedure.

GSK encourages individuals to raise privacy complaints through various available mechanisms. A privacy complaint could be registered with a line manager, a country compliance officer, a local HR or legal representative, a business unit customer service department (which includes handling privacy-related complaints), or the above country version of any of these, all of whom will independently assess the appropriate course of action in response to the complaint.

Regardless of where GSK receives data privacy complaints, if they cannot be resolved through the initial avenue, then they will be escalated as follows: first, the complaint will be escalated to the Global Privacy Team representative for the relevant business unit or department; if the complaint still cannot be resolved, it will be escalated to the Global Privacy Office for resolution. The Global Privacy Office represents the final avenue within GSK for complaint resolution. GSK endeavours to resolve complaints expeditiously and, unless exceptional circumstances apply, within six months. Individuals can contact the Global Privacy Office directly if they wish, but typically will go through the process just described. We will provide contact details of the Global Privacy Office upon request.

Accessing GSK's internal complaints procedure in no way prejudices an individual's ability to seek advice from and submit complaints to competent data protection authorities or to seek judicial remedies available via their national courts.

<u>Process and remedy for breaches outside of the EEA</u>

Where we process PII of an individual who is resident in an EEA Plus Country and a GSK company that is outside of the EEA is alleged to have breached the BCRs when processing such PII, the individual may, if the matter is not resolved satisfactorily in accordance with our complaints handling procedure, submit a complaint to a DPA or court of competent jurisdiction against the GSK company allegedly in breach in (i) the EEA country from which their PII was transferred or (ii) the United Kingdom - the location of GSK plc. If an individual brings such a claim and can demonstrate that they have suffered damage and establish facts that show that it is likely that the damage has occurred because of a breach of the BCRs, it shall be for GSK plc to prove, or to ensure that the relevant GSK company in breach proves, that such GSK entity was not in breach of its undertaking to comply with the terms of the BCRs.

If (i) a court of competent jurisdiction makes a financial award to an individual who is resident in an EEA Plus Country in relation to a breach of the BCRs by a GSK company that is outside of the EEA or (ii) a data protection authority or court makes an order against such a GSK company, and the GSK company is unable or unwilling for whatever reason to pay the financial award or comply with the order within any applicable grace period, then GSK plc shall pay the award to the individual concerned or ensure that the relevant GSK company complies with the relevant order.

9. We audit our compliance and keep our BCRs under review

GSK's Audit and Assurance group perform independent reviews of our compliance with the BCRs, which are communicated to GSK plc's Board.[10] In addition, each representative of GSK's Global Privacy Team monitors compliance within their respective areas through activities that are developed centrally by the Global Privacy Office. These monitoring activities range in frequency, depending on the risk of a particular data processing or data type, from quarterly to bi-annually. The data collected from these monitoring activities conducted across the entire organisation will be fed up to the Global Privacy Office for analysis and trending to determine whether internal controls are effective.

The Global Privacy Office will review our BCRs every 12 months to evaluate whether they comply with relevant data protection laws. If necessary, we will update or amend our BCRs following each such review to ensure continuing compliance with applicable legislation. We will notify all GSK company members of any such updates or amendments, and will provide the UK Information Commissioner's Office with an updated version of the BCRs if, since the last such update, there have been substantial changes to the BCRs that significantly affect data protection compliance, together with a brief explanation of those changes. We may update the BCRs and the list of GSK company members of the BCRs without having to reapply for an authorisation on the condition that we provide such updates and that no transfers of PII are made to a new GSK company member of the BCRs until it is effectively bound by our IGA.

10. We cooperate with Data Protection Authorities

GSK will respond openly to inquiries from any DPA regarding the application of or compliance with the BCRs or compliance with applicable laws. GSK companies will cooperate and assist one another in relation to any such inquiries or investigations, and comply with the advice of those EEA DPAs that formally approved these BCRs on any issue relating to the BCRs, unless such advice conflicts with applicable law. Where a GSK company notifies GSK plc of a conflict between applicable local law and the BCRs in accordance with rule 1, GSK plc will decide on what action to take and in cases of doubt will consult with those EEA DPAs that formally approved these BCRs. DPAs should direct inquiries to our Global Privacy Officer.

As part of GSK's commitment to assurance and risk management, GSK will also permit DPAs from which we obtain formal approval for the BCRs, upon request and subject to applicable law and respect for the confidentiality and trade secrets of the information provided, to access the results of our reviews of compliance with the BCRs and to audit our compliance.

April 2014

[10] The Audit and Assurance group in GSK is independent: the group reports through to the Chief Audit Executive, who in turn reports to the Head of Governance, Ethics and Assurance. This role reports to the CEO (and is part of GSK's Corporate Executive team), as well as to the chairman of the Audit & Risk Committee, which is made up of Board members