

Öffentliche Stellungnahme zu den verbindlichen internen Datenschutzvorschriften von GSK

Einleitung

GSKs (**wir, uns, unsere**) Aktivitäten der Personalabteilung (**HR**) sowie Forschung und Entwicklung (**F&E**) beinhalten die Verarbeitung von „persönlichen Informationen“ (siehe Glossar), einschließlich der internationalen Übermittlung dieser persönlichen Informationen. Wir haben uns beim Umgang mit persönlichen Informationen hohen Integritätsstandards verpflichtet und verbindliche interne Datenschutzvorschriften (BCRs) eingeführt, damit wir internationale Übermittlungen persönlicher Informationen innerhalb unserer Unternehmensgruppe unter Einhaltung der Datenschutzgesetze der Europäischen Union, insbesondere der Datenschutz-Grundverordnung (Verordnung 2016/679) (**DSGVO**), vornehmen können.

Was sind die BCRs?

Unsere BCRs bestehen aus mehreren Dokumenten, einschließlich unseres Datenschutzstandards und unserer Richtlinien, einer gruppeninternen Vereinbarung zwischen GSK-Unternehmen und dieser Öffentlichen Stellungnahme. Sie werden durch Schulungen und Audits unterstützt. Diese Öffentliche Stellungnahme soll die BCRs erklären und sicherstellen, dass Personen, deren persönliche Informationen wir im Kontext unserer HR- und F&E-Aktivitäten verarbeiten, (**Sie**) sich Ihrer Rechte im Rahmen der BCRs bewusst sind und wissen, wie Sie diese ausüben können.

Am Ende dieses Dokuments finden Sie ein Glossar mit den Begriffen, die in diesem Dokument verwendet werden. Sollten Sie weitere Informationen wünschen, können Sie eine Kopie unserer BCRs anfordern, indem Sie unseren EU-Datenschutzbeauftragten unter folgender Adresse kontaktieren: EU.DPO@GSK.com.

Der Geltungsbereich unserer BCRs

Die BCRs gelten für persönliche Informationen, die im Kontext unserer HR- und F&E-Aktivitäten erhoben wurden und, wie unten beschrieben, von einem GSK-Unternehmen, welches in den genehmigten EU-Ländern den Datenschutzgesetzen des Vereinigten Königreichs oder der EU unterliegt, international in ein Land außerhalb des Europäischen Wirtschaftsraums (EWR), dessen Gesetze keinen ausreichenden Schutz für persönliche Informationen bieten, übermittelt werden.

EU-Länder, in denen die Genehmigung erteilt wurde: GSK hat in folgenden Ländern eine Genehmigung für unsere BCRs erhalten: Belgien, Bulgarien, Dänemark, Deutschland, Esland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Polen, Portugal, Rumänien (nur F&E), Schweden, Schweiz, Spanien, Slowakei, Slowenien, Tschechische Republik, Ungarn, Vereinigtes Königreich, Zypern.

Unsere HR-Aktivitäten: Diese beinhalten die Administration und Verwaltung unserer Belegschaft; Einstellungs- und Vorauswahlaktivitäten; Eingehen eines Arbeitsverhältnisses, Administration von Lohn und sonstigen Arbeitgeberleistungen; Schulung, Entwicklung und Leistung; Verwaltung von Disziplinar- und Beschwerdeverfahren; Kommunikation mit Mitarbeitern und Bereitstellung von Hinweisen; Kommunikation mit Mitarbeitern bei einem Notfall; Betreuung des [Speak Up](#)-Prozesses, durch den Anliegen intern vorgebracht und gemeldet werden können; Aufrechterhaltung des Geschäftsbetriebs und Sicherstellen, dass Mitarbeiter auf Systeme zugreifen und ihre Aufgaben erfüllen können; Überprüfung und Überwachung von Mitarbeiterkommunikation; Einhaltung rechtlicher, regulatorischer und anderer uns betreffender Anforderungen, einschließlich derer, die bei Steuer-, Arbeitssicherheits-, Anti-Diskriminierungs-, Datenschutz-, Arbeits- und Zuwanderungsgesetzen und -vorschriften, Aufzeichnungs-, Melde- und Wirtschaftsprüfungspflichten und staatlichen Kontrollen anfallen; und Reaktion auf rechtliche Verfahren, Verfolgung gesetzlicher Ansprüche, Einsatz rechtlicher Mittel, Prozessverteidigung und Verwaltung interner Beschwerden und Forderungen. Die verarbeiteten persönlichen Informationen enthalten Angaben über aktuelle, ehemalige oder zukünftige GSK-Mitarbeiter oder Fremdpersonal (siehe Glossar) sowie über Ehepartner und Angehörige, falls zutreffend.

Unsere F&E-Aktivitäten: Diese beinhalten interventionistische und nicht-interventionistische klinische Studien, die allein oder teilweise von uns veranlasst, verwaltet oder finanziert werden und damit verbundene regulatorische Compliance wie Sicherheitsüberwachung und Meldung unerwünschter Ereignisse. Die verarbeiteten persönlichen Informationen enthalten Angaben im Zusammenhang mit Externen Forschern und Forschungssubjekten (siehe Glossar).

Außerhalb des Geltungsbereichs: Unsere BCRs regeln nicht die Verarbeitung und Übermittlung persönlicher Informationen durch unsere kaufmännischen Abteilungen (z.B. persönliche Informationen in Bezug auf Verbraucher, oder Personen, die in Verbindung mit den Lieferanten unserer kaufmännischen Abteilungen stehen). Diese Informationen sind durch andere gesetzliche Mechanismen geschützt. Sie umfassen nicht die Übermittlung von persönlichen Informationen durch GSK-Unternehmen mit Sitz außerhalb des EWR, die nicht den Datenschutzgesetzen des Vereinigten Königreichs oder der EU unterliegen.

GSK-Unternehmen, die von der BCR umfasst werden: Unsere BCRs sind für alle Unternehmen unserer Gruppe verbindlich, die die oben erwähnte gruppeninterne Vereinbarung unterzeichnet haben. GlaxoSmithKline plc, ein Unternehmen nach dem Recht des Vereinigten Königreichs, ist allgemein dafür verantwortlich, dass andere Unternehmen der Gruppe weltweit die BCRs einhalten, einschließlich der Behebung von Verstößen gegen die BCRs.

Unsere Regeln (wie in unserem Datenschutzstandard wiedergegeben)

1. Wir verarbeiten persönliche Informationen nach Treu und Glauben und rechtmäßig

Wir halten bei der Verarbeitung von persönlichen Informationen das anwendbare Recht ein. Im Falle eines Konflikts zwischen diesen BCRs und anwendbarem Recht, welcher voraussichtlich sehr nachteilige Auswirkungen hat, ist die Datenschutzbehörde hierüber zu informieren.

Grund für die Verarbeitung: Wir verarbeiten persönliche Informationen nur, wenn dafür ein legitimer Geschäftszweck vorliegt und die Verarbeitung für diesen Zweck erforderlich ist. Jede Verarbeitung verfügt über eine angemessene rechtliche Grundlage nach der DSGVO.

Rechtliche Grundlage für die Verarbeitung: Wir stützen uns auf die folgenden rechtlichen Grundlagen zur Verarbeitung von persönlichen Informationen. Die Verarbeitung muss erforderlich sein:

- (i) für die Erfüllung eines Vertrags, dessen Vertragspartner Sie sind, oder zur Durchführung vorvertraglicher Maßnahmen, die auf Ihre Anfrage hin erfolgen;
- (ii) um unsere rechtlichen Verpflichtungen zu erfüllen;
- (iii) für die Wahrnehmung einer Aufgabe durch uns, die im öffentlichen Interesse liegt;
- (iv) um Ihre lebenswichtigen Interessen zu schützen; oder
- (v) zur Wahrung der berechtigten Interessen von uns oder eines Dritten, sofern Ihre eigenen Interessen, Rechte und Freiheiten nicht überwiegen.

Besonderen Kategorien von Informationen: Aufgrund der Art der „besonderen Kategorien von Informationen“ (siehe Glossar) gibt es dafür zusätzliche Garantien. Wir verarbeiten besondere Kategorien von Informationen nur, wenn:

- (i) es für uns erforderlich ist, um unseren rechtlichen Pflichten nachzukommen und unsere gesetzlichen Rechte aus dem Arbeitsrecht auszuüben;
- (ii) es erforderlich ist, um Ihre lebenswichtigen Interessen zu schützen, wenn Sie aus körperlichen oder rechtlichen Gründen außer Stande sind, Ihre Einwilligung zu geben;
- (iii) die Verarbeitung persönliche Daten betrifft, die von Ihnen offensichtlich öffentlich gemacht wurden;
- (iv) es zur Geltendmachung, Ausübung und Verteidigung von Rechtsansprüchen erforderlich ist;
- (v) es aus Gründen eines erheblichen öffentlichen Interesses erforderlich ist; oder
- (vi) es für Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich entweder auf der Grundlage des anwendbaren Rechts oder aufgrund eines Vertrags mit einem Angehörigen eines Gesundheitsberufs, erforderlich ist. Unter diesen Umständen wird die Verarbeitung von einem Angehörigen eines Gesundheitsberufs vorgenommen, der einem

Berufsgeheimnis unterliegt, oder von einer anderen Person, die einer entsprechenden Geheimhaltungspflicht unterliegt.

Wir holen Ihre eindeutige Einwilligung zur Verarbeitung persönlicher Informationen und besonderer Kategorien von Informationen ein, wenn es gesetzlich vorgeschrieben ist, oder wenn wir uns nicht auf eine der oben aufgeführten Gründe stützen können.

2. Wir erheben und speichern nur das erforderliche Maß an persönlichen Informationen, um spezifische und legitime Geschäftszwecke zu verfolgen

Wir erheben nur das erforderliche Maß an persönlichen Informationen, um legitime Geschäftszwecke zu verfolgen. Wir versichern, dass diese persönlichen Informationen adäquat, relevant und nicht übermäßig sind im Verhältnis zu den Zwecken, für die wir sie erheben und/oder weiterverarbeiten. Wir greifen nach Möglichkeit auf anonymisierte Informationen statt persönliche Informationen zurück, um unsere Ziele zu erreichen. Wir stellen sicher, dass persönliche Informationen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sind.

Wir bewahren persönliche Informationen nur so lange auf, wie dies für einen legitimen Geschäftszweck erforderlich ist. Dann löschen, zerstören oder anonymisieren wir die persönlichen Informationen.

3. Wir erklären, wie persönliche Informationen genutzt werden sowie Ihre Rechte

Transparenz: Wir machen unsere Verarbeitungsaktivitäten von persönlichen Informationen transparent. Wir stellen die nach anwendbarem Recht verlangten Informationen zum Zeitpunkt der Erhebung der persönlichen Informationen zur Verfügung. Wir stellen jedenfalls die erforderlichen Mindestinformationen gemäß den Artikeln 13 und 14 DSGVO bereit. Wenn wir persönliche Informationen von Dritten statt direkt von Ihnen beziehen, kann es (abhängig vom anwendbaren Recht) sein, dass wir Ihnen diese Informationen nicht bereitstellen, sofern dies unmöglich ist oder einen unverhältnismäßigen Aufwand bedeutet.

Individuelle Rechtswahrnehmung: Wir ermöglichen Ihnen, Ihre Rechte gemäß der DSGVO wahrzunehmen, einschließlich des Rechts:

- (i) auf Auskunft zu Ihren persönlichen Informationen;
- (ii) auf Korrektur ihrer persönlichen Informationen
- (iii) auf Löschung Ihrer persönlichen Informationen;
- (iv) auf Beschränkung oder Beendigung der Verarbeitung Ihrer persönlichen Informationen;
- (v) auf Aushändigung einer Kopie Ihrer persönlichen Informationen an Sie oder an einen Dritten;
- (vi) keine automatisierten Entscheidungen über Sie zu treffen (siehe unten);
- (vii) auf Widerruf Ihrer Einwilligungserklärung; und
- (viii) dem Erhalt von Werbung zu widersprechen.

Wir halten uns auch an das anwendbare Recht von Ländern, die Ihnen andere Rechte betreffend Ihre persönlichen Informationen zusprechen. Wir können Ihr Recht auf Auskunft zu Ihren persönlichen Informationen beschränken, um andere zu schützen (z.B. das Recht einer anderen Person auf Datenschutz).

Automatisierte Entscheidungsfindung: Wir machen nur eingeschränkten Gebrauch von automatisierten Entscheidungsfindungen bei der Verarbeitung von persönlichen Informationen. Wir nutzen automatisierte Entscheidungsfindung nur, wenn:

- (i) es für den Abschluss oder die Erfüllung eines Vertrags zwischen uns und Ihnen erforderlich ist;
- (ii) es aufgrund von Rechtsvorschriften der Union oder der Mitgliedstaaten zulässig ist und die von diesen Rechtsvorschriften vorgeschriebenen Garantien implementiert wurden; oder
- (iii) Sie Ihre ausdrückliche Einwilligung erklärt haben.

4. Wir nutzen persönliche Informationen nicht für weitere Zwecke, die mit dem Zweck, für den sie ursprünglich erhoben wurden, unvereinbar sind

Zweckbindung: Wir verarbeiten persönliche Informationen nur in einer Weise, die mit dem legitimen

Geschäftszweck kompatibel ist, für den sie ursprünglich erhoben wurden. Wir benachrichtigen Sie über jeden neuen Zweck der Verarbeitung Ihrer persönlichen Informationen.

5. Wir nutzen geeignete Sicherheitsvorkehrungen

Schutz Ihrer Privatsphäre: Wir implementieren geeignete technische und organisatorische Sicherheitsmaßnahmen, um unbeabsichtigte oder unrechtmäßige Vernichtung, Verlust, Veränderung, unbefugte Offenlegung von beziehungsweise unbefugter Zugang zu persönlichen Informationen zu verhindern. Diese Maßnahmen sind angemessen zu den Risiken im Zusammenhang mit der Nutzung von persönlichen Informationen und berücksichtigen den Stand der Technik.

Umgang mit Störfällen und Verstößen: Wir benachrichtigen die Datenschutzbehörden bei Verletzungen des Schutzes personenbezogener Daten, es sei denn, dass diese Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für Ihre Rechte und Freiheiten führt. Wir benachrichtigen Sie über Verletzungen des Schutzes personenbezogener Daten, falls eine solche Verletzung voraussichtlich ein hohes Risiko für Ihre Rechte und Freiheiten darstellt und (nach unserem Ermessen) unter bestimmten anderen Umständen. Wir führen Aufzeichnungen über Verletzungen des Schutzes personenbezogener Daten, welche Einzelheiten über die Verletzung des Schutzes personenbezogener Daten, die Auswirkungen (falls vorhanden) auf Sie, uns oder andere Parteien sowie die ergriffenen Abhilfemaßnahmen zur Behebung der Verletzung enthalten. Diese Aufzeichnungen stellen wir zuständigen Datenschutzbehörden auf Anfrage zur Verfügung.

6. Wir kontrollieren die Offenlegung persönlicher Informationen an Dritte sorgfältig

Datenschutz-Management betreffend Dritte: Wir geben persönliche Informationen außerhalb unserer Unternehmensgruppe weiter, wenn dies gesetzlich vorgeschrieben ist, im Zusammenhang mit Gerichtsverfahren und in anderen beschränkten und rechtmäßigen Zusammenhängen. Wir können persönliche Informationen auch außerhalb unserer Unternehmensgruppe übermitteln, und zwar an: (a) Dritte, die in unserem Auftrag handeln, einschließlich Lieferanten; oder (b) andere unabhängige Dritte wie Forschungs- und Handelspartner oder Regulierungsbehörden.

Wenn wir auf Dritte angewiesen sind, um persönliche Informationen für uns zu verarbeiten, richten wir angemessene vertragliche, organisatorische und operative Kontrollen bei diesen Dritten ein, um die Vertraulichkeit und Sicherheit Ihrer persönlichen Informationen sicherzustellen. Wir schreiben vor, dass diese Dritten allen Bestimmungen des Artikels 28 DSGVO zustimmen. Sollten wir feststellen, dass ein Dritter persönliche Informationen auf eine Art verarbeitet, die mit unseren Anforderungen oder anwendbarem Recht unvereinbar ist, werden wir alle angemessenen Schritte unternehmen, um sicherzustellen, dass die Mängel so schnell wie möglich behoben werden.

Weiterübermittlungen an Dritte: Wenn wir persönliche Informationen international an Dritte in Ländern außerhalb des EWR übermitteln, deren Datenschutzgesetze kein angemessenes Schutzniveau für persönliche Informationen bieten, implementieren wir genehmigte Standardvertragsklauseln, deren Einzelheiten hier abrufbar sind, oder stützen uns auf einen anderen rechtmäßigen Ausnahmefall für die Übermittlung persönlicher Informationen.

Information der Behörden: Sofern gemäß anwendbaren Datenschutzgesetzen eines Mitgliedstaates erforderlich, benachrichtigen wir die zuständige Datenschutzbehörde oder holen von ihr eine Genehmigung für die Verarbeitung von persönlichen Informationen ein (einschließlich internationalen Übermittlungen persönlicher Informationen) und stellen sicher, dass die Meldungen oder Genehmigungsanträge im Falle von Änderungen aktualisiert werden.

7. Wir verfügen über ein Beschwerdeverfahren und respektieren Ihr Recht auf Rechtsmittel

Eine Beschwerde bei uns einreichen: Wenn Sie der Ansicht sind, dass wir die Regeln in unseren BCRs nicht eingehalten haben, können Sie Ihre Bedenken direkt uns gegenüber äußern und Ihre Beschwerde in unserem internen Beschwerdeverfahren prüfen lassen. Wir empfehlen Ihnen, Datenschutzbeschwerden über unser einzureichen.

HR-Aktivitäten: Mitarbeiter oder andere Personen, deren Informationen im Zusammenhang mit HR-Aktivitäten verarbeitet werden, können bei Ihrem direkten Vorgesetzten (bei GSK-Mitarbeitern), einem Landes-Compliance-Beauftragten, einem lokalen HR- oder gesetzlichen Vertreter oder deren regionaler Entsprechung eine Datenschutzbeschwerde einreichen. Diese geben die Datenschutzbeschwerde an den Beschwerdekanaal weiter, welcher die Beschwerde an die Compliance-Gruppe des Geschäftsbereichs und das Datenschutz-Kompetenzzentrum weiterleitet. Dort wird unabhängig die geeignete Vorgehensweise als Antwort auf Ihre Beschwerde bestimmt.

F&E-Aktivitäten: Personen, deren persönliche Informationen in Verbindung mit F&E-Aktivitäten verarbeitet werden, und die Forschungssubjekt sind (siehe Glossar), sollten sich an den die Studie durchführenden Mediziner oder Forscher wenden, der die Beschwerde an unser Datenschutz-Kompetenzzentrum weiterleiten wird. Wenn Sie ein Externer Forscher sind (siehe Glossar), können Sie bei dem GSK Landes-Compliance-Beauftragten, einem gesetzlichen Vertreter oder der regionalen Entsprechung eine Beschwerde einreichen. Diese werden die Datenschutzbeschwerde an den Beschwerdekanaal innerhalb GSK weiterleiten. Dort wird unabhängig die geeignete Vorgehensweise als Antwort auf Ihre Beschwerde bestimmt.

Eskalation: Unabhängig davon, wo wir Datenschutzbeschwerden erhalten, werden diese, wenn sie nicht gelöst werden können, folgendermaßen eskaliert: (i) an den GSK Landes-Datenschutz-Ansprechpartner, dessen Kontaktangaben auf unserer Webseite [hier](#) veröffentlicht sind; oder (ii) dann an den EU-Datenschutzbeauftragten von GSK unter EU.DPO@GSK.com. Der EU-Datenschutzbeauftragte stellt innerhalb GSK die letzte Stelle zur Beschwerdelösung im Zusammenhang mit unseren BCRs dar. Wir bemühen uns, Beschwerden zügig zu lösen und GSK wird Sie, sofern keine außergewöhnlichen Umstände vorliegen, innerhalb eines Monats nach Erhalt der Beschwerde schriftlich kontaktieren. Diese Mitteilung wird entweder: (a) unsere Position in Bezug auf die Beschwerde und jegliche Maßnahmen, die wir als Antwort auf die Beschwerde ergriffen haben oder ergreifen werden, darlegen; oder (b) angeben, wann Sie über unsere Position informiert werden, was anschließend nicht länger als zwei Monate dauert. Wenn Sie möchten, können Sie unseren EU-Datenschutzbeauftragten direkt kontaktieren.

Eine Beschwerde bei einer Datenschutzbehörde oder vor Gericht einreichen: Sie können bei folgenden Instanzen Beschwerde einreichen: (i) der zuständigen Datenschutzbehörde des Landes, in dem Sie ihren Hauptwohnsitz haben, arbeiten oder der angebliche Verstoß stattgefunden hat, (ii) dem Datenschutzbeauftragten des Vereinigten Königreichs (Information Commissioner) oder Gerichten im Vereinigten Königreich (dem Standort von GlaxoSmithKline plc); (iii) den Gerichten des EWR-Landes, aus welchem wir Ihre persönlichen Informationen übermittelt haben; und (iv) den Gerichten im EWR-Land, in dem Sie ihren Hauptwohnsitz haben. Die Befolgung unseres internen Beschwerdeprozesses beeinträchtigt Ihr Recht, diese Möglichkeiten zu nutzen, in keinsten Weise.

[Juni 2018]