Grundsätze für die Compliance im Bereich des Daten- und Geheimhaltungsschutzes

Verantwortlich	Nicolas Passadelis, Leiter Data Governance (GSB-DGO)
Referenz	Direktive Data Governance vom 1. Dezember 2016
Genehmigung	Martin Vögeli, Leiter Group Strategy & Board Services (GSB)
Inkrafttreten	1. Mai 2018

1 Zweck

Die Grundsätze für die Compliance im Bereich des Daten- und Geheimhaltungsschutzes einschliesslich allfälliger Anhänge ("**Compliance-Grundsätze**") legen die Anforderungen für die Verarbeitung von Daten fest. Sie definieren die Aufbau- und Ablauforganisation sowie die dazu erforderlichen Rollen und Zuständigkeiten.

Diese Grundsätze dienen dem Nachweis der Sicherstellung der Compliance und ist entsprechend öffentlich. Sie kann Behörden, Kunden oder sonst interessierten Dritten jederzeit zugestellt werden.

2 Definition

Für die Zwecke dieser Compliance-Grundsätze werden bestimmte Begriffe wie folgt definiert:

Anforderungen:	Regeln und Einschränkungen für die Verarbeitung von Daten basierend auf gesetzlichen und/oder vertraglichen Vorschriften, spezifischen Kundenweisungen und internen Vorgaben;
Betroffene Person:	Natürliche Person, deren personenbezogene Daten verarbeitet werden;
Daten:	Elektronische Informationen jeglicher Art, die im Rahmen der Unternehmens- und Geschäftstätigkeit von Swisscom verarbeitet werden;
Personenbezogene Daten:	Daten, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen;
Swisscom:	Swisscom AG und Swisscom (Schweiz) AG
Swisscom-Konzern:	Swisscom und die Konzerngesellschaften
Verarbeitung:	Jegliche Form der Bearbeitung von Daten einschliesslich Erhebung, Erfassung, Zugriff, Organisation, Speicherung, Abfrage, Anpassung,

Veränderung, Verknüpfung, Übermittlung, Weitergabe, Offenlegung, Anonymisierung/ Pseudonymisierung, Löschung oder Vernichtung unabhängig davon, ob sie manuell oder automatisch erfolgt.

3 Geltungsbereich

Diese Compliance-Grundsätze gelten für die Swisscom AG und Swisscom (Schweiz) AG. Sie sind auf jegliche Verarbeitung von Daten anwendbar. Diese Compliance-Grundsätze finden somit insbesondere Anwendung auf:

- Alle Daten, die durch, bzw. durch Dritte im Auftrag von Swisscom AG oder Swisscom (Schweiz) AG verarbeitet werden;
- Alle Daten, die von Swisscom AG und Swisscom (Schweiz) AG aktuell oder in Zukunft verarbeitet werden, und zwar unabhängig davon, ob diese Daten noch produktiv oder inzwischen nutzlos geworden sind;
- Jegliche Art der Verarbeitung von Daten, und zwar unabhängig davon, wie diese Daten bearbeitet werden.

4 Vorbehalt des anwendbaren Rechts

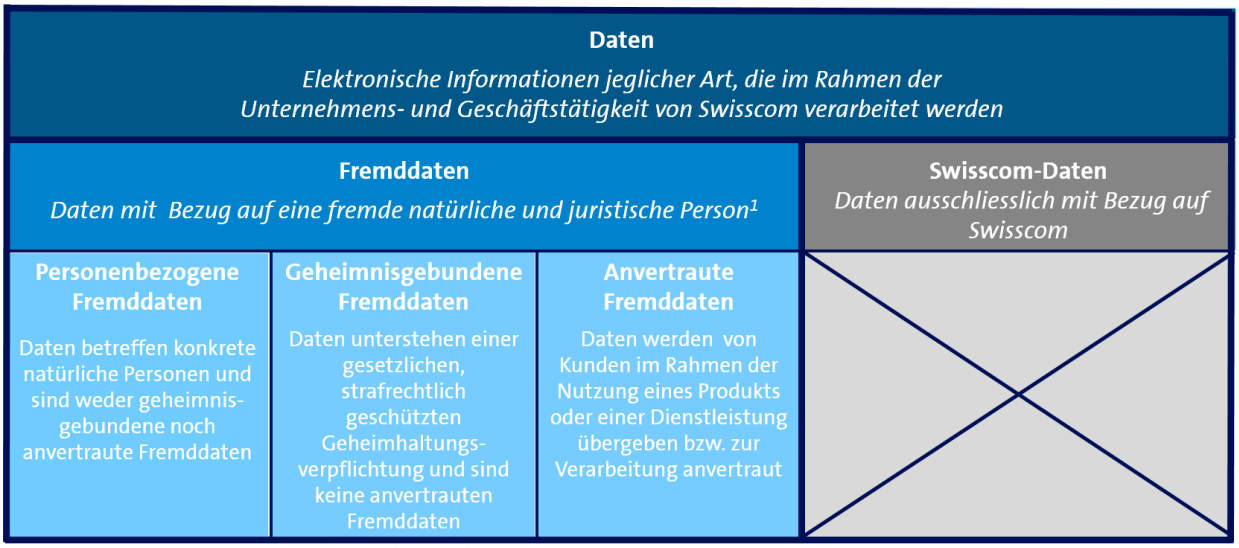
Die Geltung dieser Compliance-Grundsätze steht unter dem Vorbehalt des anwendbaren Rechts. Sollten einzelne Bestimmungen dieser Compliance-Grundsätze dem geltenden in- oder ausländischen Recht widersprechen, so geniesst das anwendbare Recht Vorrang.

5 Datenarten

Daten sind nicht gleich Daten. Daten unterscheiden sich ganz erheblich voneinander, sei es, weil sie verschiedene Personen betreffen, unterschiedliche Inhalte aufweisen oder in unterschiedlichen Geschäftsprozessen verarbeitet werden. Hinzu kommt, dass die Anforderungen und auch der Schutzbedarf je nach Art der Daten unterschiedlich ausfallen kann.

Es ist deshalb erforderlich, Daten in verschiedene Datenarten einzuteilen, um die unterschiedlichen Eigenschaften von Daten und die Anforderungen für deren Verarbeitung sichtbar zu machen und deren Einhaltung sicherstellen zu können.

Aus diesem Grund werden bei Swisscom folgende zwei grundlegende Datenarten unterschieden: (1) Fremddaten und (2) Swisscom-Daten. Fremddaten werden zusätzlich in drei Unterarten unterteilt. In der Übersicht lassen sich die Datenarten bei Swisscom wie folgt darstellen:



[1] *Als natürliche Person bezeichnet man einen lebenden Menschen als Träger von Rechten und Pflichten. Als juristische Person bezeichnet man eine Personenvereinigung, die selbst Träger von Rechten und Pflichten sein kann. Unternehmen wie Aktiengesellschaften oder Gesellschaften mit beschränkter Haftung (GmbH) sind beispielsweise juristische Personen.*

5.1 Fremddaten

Als Fremddaten werden Daten bezeichnet, die einen Bezug zu einer fremden natürlichen oder juristischen Person aufweisen. Fremd sind alle natürlichen und juristischen Personen mit Ausnahme von Swisscom AG und Swisscom (Schweiz) AG. Somit kann die fremde Person innerhalb von Swisscom sein (z.B. Mitarbeiter) oder ausserhalb (z.B. Lieferant, Privat- oder Geschäftskunde). Es kommt nicht darauf an, ob dieser Bezug operativer, kommerzieller, vertraglicher oder sonst wie rechtlicher Natur ist. Entscheidend ist, dass die natürliche oder juristische Person, die durch die Verarbeitung der Fremddaten durch Swisscom in irgendeiner Weise betroffen ist und dadurch einen rechtlichen Schutz geniesst, der die Verarbeitung dieser Daten durch Swisscom rechtlich beschränkt.

- Personenbezogene (einfache) Fremddaten: Bei einfachen Fremddaten handelt es sich um Daten, welche stets eine konkrete natürliche oder juristische Person betreffen und weder geheimnisgebundene Fremddaten noch anvertraute Fremddaten darstellen. Einfache Fremddaten stellen damit stets personenbezogene Daten dar und fallen unter die anwendbaren Datenschutzgesetze. Einfache Fremddaten können sich dabei auf Privatkunden, Mitarbeiter von Swisscom, Mitarbeiter von Geschäftskunden, Mitarbeiter von Lieferanten und Geschäftspartner oder andere natürlichen Personen ausserhalb von Swisscom beziehen.

- Geheimnisgebundene (qualifizierte) Fremddaten: Bei geheimnisgebundene Fremddaten handelt es sich um Fremddaten, welche keine anvertrauten Fremddaten sind und einer gesetzlichen Geheimhaltungsverpflichtung unterstehen, deren Verletzung strafrechtlich ge-

ahndet werden kann. Geheimnisgebundene Fremddaten unterstehen vor allem dem Fernmeldegeheimnis (z.B. Call Record Data bzw. "CDR" oder der Inhalt einer SMS") oder anderen gesetzlichen Geheimhaltungspflichten.

- Anvertraute Fremddaten: Diese Daten werden Swisscom von ihren Privat- und Geschäftskunden (Grosskunden und KMU) im Rahmen der Nutzung eines Produkts oder einer Dienstleistung übergeben bzw. zur Verarbeitung anvertraut (z.B. im Rahmen eines Hostings). Swisscom verarbeitet die anvertrauten Fremddaten auf der Basis eines Vertragsverhältnisses im Auftrag und Interesse des Kunden. Anvertraute Fremddaten können sowohl technische und operative Daten als auch personenbezogene Daten enthalten.

5.2 Swisscom-Daten

Als Swisscom-Daten werden Daten bezeichnet, die (anders als Fremddaten) keinerlei Bezug zu einer konkreten fremden natürlichen oder juristischen Person aufweisen. Swisscom-Daten weisen also ausschliesslich einen Bezug zu den Gesellschaften Swisscom AG bzw. Swisscom (Schweiz) AG auf (z.B. Finanzzahlen, Sach- und technische Daten).

6 Anforderungen

Je nach Datenart und Art der Verarbeitung sind von Swisscom bei der Verarbeitung von Daten unterschiedliche Anforderungen einzuhalten. Diese Anforderungen können sich aus gesetzlichen und/oder vertraglichen Vorschriften, Kundenweisungen und internen Vorgaben der Organisationseinheit Data Governance ergeben. Die Anforderungen sind ungeachtet ihrer Quelle stets verbindlich und im Rahmen ihrer jeweiligen Anwendbarkeit bei jeglicher Verarbeitung von Daten zu beachten. Ausnahmen sind vom Leiter Data Governance zu bewilligen.

6.1 Gesetzliche Vorschriften

6.1.1 Datenschutzgesetze

Daten, welche Swisscom im Rahmen ihrer Geschäftsaktivitäten verarbeitet, enthalten sehr oft personenbezogene Daten. Die Verarbeitung von personenbezogenen Daten wird in der Regel durch verschiedene Datenschutzgesetze auf supranationaler[1], nationaler[2] oder kantonaler Ebene reguliert.

[1] Verordnung der EU vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr (Datenschutz-Grundverordnung; DSGVO); Verordnung der EU über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation (Verordnung über Privatsphäre und elektronische Kommunikation; ePrivacy-Verordnung);

[2] Bundesgesetz über den Datenschutz vom 19. Juni 1992 (DSG).

Ziel der Datenschutzgesetzgebung ist es, die Persönlichkeit einer natürlichen Person zu schützen, deren personenbezogene Daten verarbeitet werden. Die betroffene Person hat das Recht, über die Verarbeitung ihrer personenbezogenen Daten selbst zu entscheiden und vor einem Missbrauch ihrer Daten geschützt zu werden. Die Datenschutzgesetze regeln deshalb ausführlich, unter welchen Voraussetzungen personenbezogene Daten verarbeitet werden dürfen. Nur in Ausnahmefällen ist eine Verarbeitung von Daten auch gegen den Willen der betroffenen Person zulässig.

6.1.2 Geheimhaltungsgesetze

Swisscom verarbeitet im Rahmen ihrer Geschäftsaktivitäten sehr oft Daten, die einer gesetzlichen Geheimhaltungsverpflichtung[3] unterliegen. Auch wenn sich die gesetzlichen Geheimhaltungsverpflichtungen je nach Art des geschützten Geheimnisses und Person des Geheimnisherrn in ihren rechtlichen Auswirkungen unterscheiden, so ist ihnen doch gemeinsam, dass sie Umfang und Zweck der Verarbeitung von gesetzlich geschützten Geheimnissen rechtlich einschränken und jeder Person, die berechtigterweise Zugang zu einem Geheimnis erhält, die Pflicht auferlegt, das Geheimnis zu bewahren und angemessene Massnahmen zum Schutz des Geheimnisses zu treffen.

6.2 Vertraglich vereinbarte Geheimhaltung

Die Pflicht zur Geheimhaltung von Daten bzw. die Konkretisierung gesetzlicher Geheimhaltungsverpflichtungen können sich auch aus vertraglichen Vereinbarungen oder sonstigen Abreden ergeben, welche Swisscom im Verhältnis zu Dritten eingeht. Die überwiegende Mehrheit der Geschäftsbeziehungen, welche Swisscom mit Dritten eingeht, verpflichten Swisscom zur Geheimhaltung von Informationen, welche sie im Zusammenhang mit dieser Geschäftsbeziehung von den betreffenden Dritten erhält. Neben der Pflicht zur Geheimhaltung schränken auch Geheimhaltungs- bzw. Vertraulichkeitsvereinbarungen oder sonstige Abreden regelmässig auch den Umfang und Zweck der Verarbeitung von (oft vertraglich definierten) Geheimnissen stark ein oder legen Bedingungen für Verarbeitung von Daten fest (z.B. Datenverarbeitung in der Schweiz, sicherheitsgeprüfte Mitarbeitende oder Genehmigungspflicht für Subunternehmen). Geheimnisse dürfen in der Regel nur zur Erfüllung der vertraglich vereinbarten Leistungen verwendet werden. Eine anderweitige Verwendung ist untersagt.

6.3 Spezifische Kundenweisungen

Die Regeln und Einschränkungen, welche bei der Verarbeitung von Daten beachtet werden müssen, können auch auf spezifische Kundenweisungen beruhen. Diese Weisungen können von Personen kommen, welche von der Datenverarbeitung direkt oder indirekt betroffen sind. Dies gilt insbesondere für Privat- und Geschäftskunden. Das Recht auf Erteilung von spezifischen Kundenweisungen kann gesetzlicher oder vertraglicher Natur sein.

---

[3] Z.B. Berufsgeheimnis gemäss Art. 321 f. StGB; Amtsgeheimnis gemäss Art. 320 StGB; Geschäftsgeheimnis gemäss Art. 162 StGB; Bankkundengeheimnis gemäss Art. 47 BankG; Post- und Fernmeldegeheimnis gemäss Art. 43 FMG/Art. 321ter StGB; Berufsgeheimnis der Finanzmarktinfrastruktur gemäss Art. 147 FinfraG; Wirtschaftlicher Nachrichtendienst gemäss Art. 273 StGB.

6.4 Interne Vorgaben

Anforderungen für die Verarbeitung von Daten können sich im Anwendungsbereich dieser Compliance-Grundsätze auch aus internen Vorgaben der Organisationseinheit Data Governance ergeben. Diese Vorgaben können in Form von Policies, Weisungen oder Richtlinien erlassen werden oder ad-hoc erfolgen, so beispielsweise im Rahmen einer konkreten Beratung oder Überprüfung. Sämtliche Vorgaben der Organisationseinheit Data Governance sind grundsätzlich verbindlich, sofern der Leiter Data Governance auf die Verbindlichkeit nicht ausdrücklich verzichtet.

7 Data Governance-System der Swisscom

7.1 Definition

Das Data Governance-System von Swisscom (DGS) besteht aus der Gesamtheit aller dokumentierten Strukturen, Vorgaben, Massnahmen und Prozesse zur systematischen Etablierung und Förderung einer Datenkultur mit dem Ziel der Sicherstellung einer strategischen und rechtskonformen sowie legitimen Verarbeitung von Daten bei Swisscom.

7.2 Elemente

Das DGS von Swisscom umfasst folgende Elemente:

- Datenkultur
- Schutzziele
- Risikomanagement
- Organisation
- Kommunikation und Information
- Überwachung und Verbesserung

7.3 Datenkultur

Die Datenkultur von Swisscom bezeichnet die kulturellen Grundlagen und Begebenheiten für eine Nutzung von Daten in Übereinstimmung mit diesen Compliance-Grundsätzen und insbesondere mit den Anforderungen.

7.4 Schutzziele

Das DGS von Swisscom ist einer Reihe von Schutzzielen verpflichtet. Die allgemeinen Schutzziele gelten für jede Form der Datenverarbeitung unabhängig von der Datenart. Unbeachtlich ist auch, in welchem Stadium des Lebenszyklus von Daten die Verarbeitung stattfindet.

Es werden folgende Kategorien von Schutzzielen unterschieden:

7.4.1 Allgemeine Schutzziele

7.4.1.1 Rechtmässigkeit – Verarbeitung stets in Übereinstimmung mit dem anwendbaren Recht

Es ist sicherzustellen, dass die Verarbeitung von Daten zu keinem Zeitpunkt gegen eine anwendbare rechtliche bzw. vertragliche Vorschrift verstösst.

7.4.1.2 Datenrichtigkeit – Verarbeitung nur von aktuellen und richtigen Daten

Bei jeglicher Datenverarbeitung ist generell sicherzustellen, dass nur aktuelle und inhaltlich richtige Daten verarbeitet werden.

7.4.1.3 Datensicherheit – Gewährleistung von Datenvertraulichkeit, -verfügbarkeit und -integrität

Die Vertraulichkeit, Verfügbarkeit und Integrität von Daten müssen zu jedem Zeitpunkt und über den gesamten Lebenszyklus hinweg risikogerecht gewährleistet sein.

7.4.2 Spezifische Schutzziele für personenbezogene und geheimnisgebundene Daten

7.4.2.1 Transparenz – Angemessene Information der betroffenen Personen

Werden personenbezogene oder geheimnisgebundene Daten innerhalb von Swisscom erhoben, so ist sicherzustellen, dass die betroffene Person über die Details der Datenverarbeitung durch Swisscom angemessen informiert wird.

Liegt die Quelle der Daten ausserhalb von Swisscom, so ist vor Erlangung der Kontrolle über die Daten und jeglicher weiteren Verarbeitung der Daten durch Swisscom zu prüfen, ob die betroffenen Personen auch über die Art der von Swisscom beabsichtigte Verarbeitung ihrer Daten angemessen informiert worden sind.

7.4.2.2 Zweckbindung – Verarbeitung nur für rechtmässige Zwecke

Personenbezogene und geheimnisgebundene Fremddaten dürfen nur für die Zwecke verarbeitet werden, über welche die betroffene Person informiert wurde. Das bedeutet, dass die angestrebten Verarbeitungszwecke schon bei der Erhebung bekannt sind und transparent gemacht werden. Ändern sich nach erfolgter Information die transparent gemachten Verarbeitungszwecke oder treten

neue Verarbeitungszwecke hinzu, so ist eine Verarbeitung der personenbezogenen Daten für diese veränderten oder neuen Zwecke ohne Sicherstellung einer neuen Rechtsgrundlage nicht gestattet.

7.4.2.3 Rechtsgrundlage – Verarbeitung nur auf einer gesicherten Rechtsgrundlage

Die Verarbeitung von personenbezogenen und geheimnisgebundenen Fremddaten ist nur zulässig, wenn sie auf einer gesicherten Rechtsgrundlage erfolgt. Die zulässigen Rechtsgrundlagen ergeben sich aus den anwendbaren Datenschutz- bzw. Geheimnisschutzgesetzen und erfassen insbesondere Fälle:

- Die Verarbeitung betrifft die Daten einer natürlichen Person und dient dazu, einen Vertrag mit dieser natürlichen Person abzuschliessen, zu erfüllen oder durchzusetzen;
- Die Verarbeitung betrifft die personenbezogenen Daten einer natürlichen Person, die zu dieser Verarbeitung ihre Einwilligung erteilt hat;
- Die Verarbeitung erfolgt ausschliesslich zur Erfüllung einer Rechtspflicht von Swisscom;
- Die Verarbeitung ist für den Schutz lebenswichtiger Interessen einer natürlichen Person erforderlich.

Kann eine Verarbeitung auf keine der oben genannten Rechtsgrundlagen gestützt werden, so muss sie rechtlich genauer geprüft und durch den Leiter Data Governance autorisiert werden.

7.4.2.4 Datenminimierung – Möglichst sparsame Verarbeitung

Bei der Verarbeitung von personenbezogenen und geheimnisgebundenen Daten ist darauf zu achten, dass sowohl der Umfang der erhobenen Personendaten als auch die jeweils durchgeführten Verarbeitungsschritte auf ein Minimum beschränkt werden. Der Grundsatz der Datensparsamkeit ist erfüllt, wenn nur jene Daten erhoben werden, welche zur Erreichung des Zwecks, für den sie erhoben werden, erforderlich sind. Es gilt der Grundsatz "so viel Verarbeitung wie nötig und so wenig Verarbeitung wie möglich". Der Grundsatz der Datensparsamkeit lässt sich folglich nur einhalten, wenn man die Verarbeitungszwecke, für welche die Personendaten erhoben werden sollen, bereits vor der Datenerhebung festgelegt hat. Der Grundsatz der Datenminimierung verlangt auch, dass Zugriffe auf personenbezogene Daten auf das erforderliche Mass beschränkt bleiben.

7.4.2.5 Betroffenenrechte – Konsequente Erfüllung der gesetzlichen Rechte betroffener Personen

Den von der Verarbeitung ihrer personenbezogenen Daten betroffenen Personen stehen eine Reihe von datenschutzrechtlichen Ansprüchen zu, die sie jederzeit gegenüber einem verantwortlichen Datenverarbeiter geltend machen können.

7.4.2.6 Datenlöschung – Rechtskonforme Löschung

In zeitlicher Hinsicht dürfen Personendaten nur solange gespeichert werden, wir dies erforderlich ist, um den Zweck zu erreichen, für welchen die Daten erhoben wurden. Ist dieser Zweck erreicht, müssen die Daten grundsätzlich gelöscht werden.

7.4.3 Spezifische Anforderungen für geheimnisgebundene Fremddaten

7.4.3.1 Vertragserfüllung – Verarbeitung ohne Einwilligung bzw. Anonymisierung nur zur Vertragserfüllung

Geheimnisgebundene Fremddaten unterliegen einer gesetzlichen Nutzungsbeschränkung und dürfen grundsätzlich nur verarbeitet werden, um die vereinbarten Dienstleistungen zu erbringen und diese gegenüber dem Kunden abzurechnen. Für andere Zwecke dürfen geheimnisgebundene Daten nur verarbeitet werden, wenn die betroffene Person vorgängig eingewilligt hat oder wenn die geheimnisgebundenen Daten vor einer Verarbeitung für andere Zwecke anonymisiert worden sind.

7.4.3.2 Weisungsgebundenheit – Einhaltung von Kundenweisungen bei Verarbeitung

Die betroffenen Personen sind mit Bezug auf die Verarbeitung von geheimnisgebundenen Daten jeweils weisungsbefugt. Die Weisungen der betroffenen Personen mit Bezug auf die Verarbeitung der geheimnisgebundenen Daten sind grundsätzlich zu befolgen.

7.4.4 Spezifische Anforderungen für anvertraute Daten

7.4.4.1 Vertragserfüllung – Verarbeitung ausschliesslich zur Vertragserfüllung

Anvertraute Fremddaten dürfen ausschliesslich zum Zwecke der Erfüllung und nach Massgabe des Vertrages mit dem betreffenden Privat- oder Geschäftskunden verarbeitet werden.

7.4.4.2 Weisungsgebundenheit – Einhaltung von Kundenweisungen bei Verarbeitung

Die betreffenden Privat- oder Geschäftskunden sind mit Bezug auf die Verarbeitung der von ihnen anvertrauten Daten weisungsbefugt. Die Weisungen der berechtigten Privat- oder Geschäftskunden mit Bezug auf die Verarbeitung der von ihnen anvertrauten Daten sind grundsätzlich zu befolgen.

7.5 Risikomanagement

7.5.1 Zielsetzung

Der Schutz des Swisscom-Konzerns, seiner Organe und Mitarbeitenden vor Unternehmensrisiken wie rechtliche Sanktionen, finanzielle Verluste und Reputationsschäden (**Unternehmensrisiken**) stellt eine Zielvorgabe des Verwaltungsrates dar. Auf Grundlage dieser Zielvorgabe werden unter

Berücksichtigung der Risikobeurteilung die Massnahmen zur Sicherung und Überwachung der Compliance festgelegt.

Neben der angemessenen Berücksichtigung von Unternehmensrisiken erfordert die Anwendung und Einhaltung von Anforderungen an die Verarbeitung von Daten auch eine kontinuierliche Ermittlung und Bewertung der Risiken für die Rechte und Freiheiten von natürlichen Personen (**Datenschutzrisiken**). Datenschutzrisiken sind bei der Festlegung von Massnahmen zur Etablierung und Förderung einer Datenkultur deshalb ebenfalls angemessen zur berücksichtigen.

7.5.2 Elemente des Risikomanagements

Das Risikomanagement des DGS erfasst folgende Elemente:

- Zielfestlegung
- Ereignisidentifikation;
- Risikobeurteilung;
- Kontrollaktivitäten;
- Information und Kommunikation;
- Überwachung.

7.6 Organisation

7.6.1 Organisationsmodell

Das Organisationsmodell des DGS zeichnet sich aus durch die Zusammenarbeit von Linien und transversalen Funktionen unter der strategischen Führung und Koordination der Organisationseinheit Data Governance (DGO).

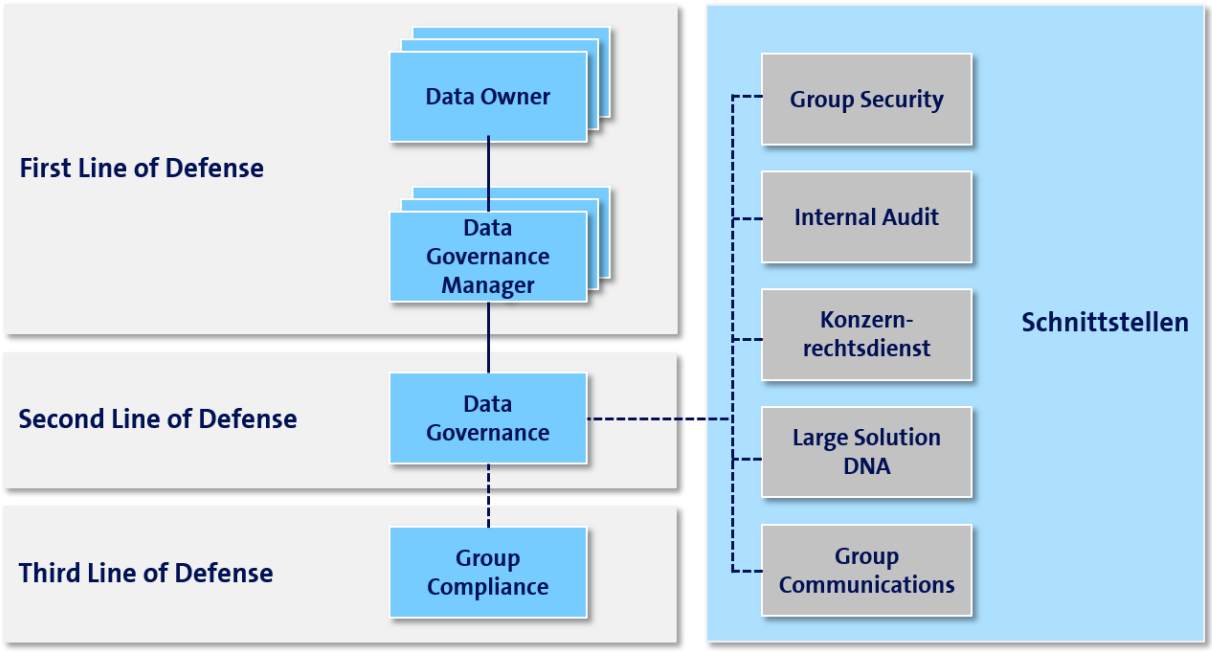
Zur Sicherstellung einer rechtskonformen sowie legitimen Verarbeitung von Daten bei Swisscom weist das Organisationsmodell ein dreistufiges Kontroll- und Überwachungssystem auf (*Three Lines of Defense-Modell).* Die drei Stufen sind:

- First Line of Defense: Data Owners und Data Governance Managers;
- Second Line of Defense: Funktion Data Governance und interner Datenschutzbeauftragter;
- Third Line of Defense: Group Compliance.

Zur Unterstützung der Etablierung und Förderung der Datenkultur in den einzelnen Geschäftsbereichen unterhält DGO zudem enge Beziehungen zu folgenden Schnittstellenfunktionen:

- Large Solution Data, Analytics & AI;
- Group Security;
- Konzernrechtsdienst;
- VR-Internal Audit;
- Group Communications & Responsibility.

Das Organisationsmodell lässt sich wie folgt darstellen:



7.7 Rollen und Verantwortlichkeiten

7.7.1 Mitarbeiter und Partner

Mitarbeiter jeglicher Stufe und Funktion sowie externe Partner sind in ihrem Zuständigkeitsbereich für Einhaltung der Anforderungen verantwortlich. Im Falle von Unklarheiten oder Fragen können sich die betreffenden Führungskräfte und Mitarbeiter an den zuständigen Data Governance Manager oder den Konzernrechtsdienst wenden.

7.7.2 Data Owners

Data Owners tragen in ihrem Zuständigkeitsbereich die Verantwortung für die Überwachung der Risiken (Risk Owner) und für die Umsetzung von Anforderungen im Bereich Data Governance. Sie

tragen die rechtliche und kommerzielle Verantwortung und stellen die erforderlichen organisatorischen und finanziellen Ressourcen bereit. Ihre Verantwortung erfasst insbesondere:

- Festlegung von Organisation, Verantwortlichkeiten und Prozessen für die Einhaltung der Anforderungen im Bereich Data Governance in ihrem Zuständigkeitsbereich;
- Ernennung, Instruktion und Beaufsichtigung der Data Governance Managers in ihrem Zuständigkeitsbereich.

Jeder Unternehmensbereich ernennt mindestens einen Data Owner. Die Ernennung erfolgt in Absprache mit DGO. Der Data Owner bildet zusammen mit den Data Governance Managers die First Line of Defense.

7.7.3 Data Governance Managers

Data Governance Managers sind dafür verantwortlich, dass Daten in ihrem Zuständigkeitsbereich in Übereinstimmung mit sämtlichen Anforderungen verarbeitet werden. Ihre Verantwortung erfasst in ihrem Zuständigkeitsbereich insbesondere:

- Autorisierung und Kontrolle des Zugangs zu Daten;
- Gewährleistung der Datensicherheit;
- Durchführung von Datenschutz-Folgeabschätzungen;
- Dokumentation der Datenverarbeitung;
- Periodische Überprüfung der Wirksamkeit der Umsetzung von Anforderungen in ihrem Zuständigkeitsbereich;
- Unverzügliche Meldung von erfolgten oder potentiellen Verletzungen von Anforderungen im Bereich des Daten- und Geheimnisschutzes an DGO;
- Eskalation von Fragen, Entscheidungen und Problemen, die vom zuständigen Data Owner nicht oder nicht zufriedenstellend gelöst werden können, an DGO;
- Periodische Berichterstattung über die Verarbeitung in ihrem Zuständigkeitsbereich an DGO;

Im Interesse einer effektiven und wirksamen Wahrnehmung ihrer Aufgaben nach Massgabe dieser Data Governance Compliance-Grundsätze sollten Data Governance Manager folgende persönlichen Voraussetzungen erfüllen:

- Direkte oder indirekte Entscheidungsbefugnisse mit Bezug auf die Verarbeitung von Daten in ihrem Zuständigkeitsbereich;

- Ausreichende Zeitressourcen und leichte Erreichbarkeit;
- Gute Kenntnisse über Geschäftsprozesse, technische Verfahren und Datenmodellierungen in ihrem Zuständigkeitsbereich;
- Interesse an datenschutzrechtlichen Zusammenhängen in ihrem Zuständigkeitsbereich;
- Bereitschaft zur Wahrnehmung einer Schnittstellenfunktion zwischen ihrem Zuständigkeitsbereich und DGO;
- Erfahrung in Fragestellungen der digitalen Transformation bzw. Verarbeitung von Daten.

7.7.4 Data Governance

Die Organisationseinheit Data Governance ist Teil des Assurance Framework des Swisscom-Konzerns. Sie legt die Aufbau- und Ablauforganisation zur Etablierung und Förderung der Datenkultur und ist der Einhaltung von Rechtsvorschriften verpflichtet. Data Governance bildet die Second Line of Defense.

Basierend auf der Direktive Data Governance [1] umfassen die Verantwortlichkeiten der Organisationseinheit Data Governance folgende Kerntätigkeiten:

Kompetenz

- Rechtsbeobachtung: Kontinuierliche Verfolgung und Validierung von Rechtsentwicklungen im Bereich des Daten- und gesetzlichen bzw. vertraglichen Geheimhaltungsschutzes;
- Rechtsanalyse: Analyse der Relevanz von Rechtsentwicklungen für Swisscom und Berichte über relevante Rechtsentwicklungen an interne Stakeholder;
- Massnahmendefinition: Definition und Dokumentation von Massnahmen zur Umsetzung von relevanten Rechtsentwicklungen;
- Weiterbildung: Kontinuierliche Weiterentwicklung von Rechtskompetenzen bei DGO durch Selbst- und Teamstudium;

Steuerung

- Risikomanagement: Identifikation, Bewertung, Steuerung und Darstellung von Unternehmens- und Datenschutzrisiken bei der Verarbeitung von Daten;
- Vorgaben: Erlass von internen Vorgaben (wie Policies, Weisungen oder Richtlinien) zur Steuerung von Datenverarbeitungen bei Swisscom;

- Schulung: Definition und Durchführung von Schulungsmassnahmen zur Einhaltung von Anforderungen;
- Überprüfung: Überprüfung der Einhaltung von Vorgaben und der Wirksamkeit von internen Vorgaben und Schulungen;

Kommunikation

- Datenkultur: Entwicklung und Umsetzung von kommunikativen Massnahmen zur Etablierung und Förderung der Datenkultur;
- Open Data: Gesamtverantwortung für die Open Data-Plattform von Swisscom und deren Kommunikation gegen innen und aussen. Die Freigabe von Open Data-Datensätzen erfolgt durch den Leiter Group Strategy and Board Services;
- Externes Stakeholdermanagement: Pflege der Beziehungen zu externen Personen und Gruppen (einschliesslich Behörden), welche die Nutzung von Daten innerhalb von Swisscom beeinflussen können oder potentiell davon betroffen sind;
- Öffentlichkeitsarbeit: Medien- und Öffentlichkeitsarbeit mit Bezug auf die digitale Transformation und Datennutzung durch Swisscom;

Beratung

- Strategische Projekte: Beratung zu Fragen des Daten- und gesetzlichen bzw. vertraglichen Geheimhaltungsschutzes bei internen Projekten mit strategischer Bedeutung sowie Freigabe solcher Projekte. Von strategischer Bedeutung sind Projekte, welche:
  - Potentiell ein überdurchschnittliches Compliance-, Datenschutz- und/oder Reputationsrisiko für Swisscom mit sich bringen;
  - Bei Behörden, die Mehrzahl oder Gesamtheit von Privatkunden oder Geschäftskunden, den Medien und/oder in der Öffentlichkeit eine besondere Aufmerksamkeit finden können;
  - Datenverarbeitungsmethoden, Technologien oder Anwendungen betreffen, deren rechtliche Beurteilung noch nicht gesichert ist; oder
  - Die Verarbeitung von personenbezogenen Daten der Mehrzahl oder Gesamtheit der Mitarbeitenden von Swisscom betreffen.

  DGO kann die Beratung bei internen Projekten mit strategischer Bedeutung im Einzelfall an den Konzernrechtsdienst delegieren.

- Interne Stakeholder: Beratung von internen Stakeholdern bei Fragen zum Daten- und gesetzlichen bzw. vertraglichen Geheimhaltungsschutz;
- Self-Service: Auf- und Ausbau von Selbstberatungskompetenzen und -mitteln zur Einhaltung der Anforderungen mit Bezug auf die Verarbeitung von Daten;
- Rechtsstreitigkeiten: Führung von Rechtsstreitigkeiten mit hauptsächlichem Fokus auf Fragen des Daten- und gesetzlichen Geheimhaltungsschutzes in Absprache mit dem Konzernrechtsdienst. Unterstützung des Konzernrechtsdiensts in anderen Rechtsstreitigkeiten mit Rechtsfragen zum Daten- und gesetzlichen bzw. vertraglichen Geheimhaltungsschutz.

Interner Datenschutzbeauftragter

Der Leiter Data Governance nimmt die Funktion des internen Datenschutzbeauftragten wahr. Er führt diese Funktion unabhängig und frei von Interessenskonflikten aus. Er ist dabei stets dem rechtmässigen und legitimen Umgang mit Daten verpflichtet. Im Rahmen seiner Zuständigkeit verfügt er über ein uneingeschränktes Auskunfts-, Zugangs- und Einsichtsrecht sowie ein Weisungsrecht. Der interne Datenschutzbeauftragte berichtet zur Sicherstellung einer unabhängigen Beurteilung seiner Tätigkeit mindestens jährlich an den Verwaltungsrat.

7.8 Schnittstellenfunktionen

7.8.1 Group Security

Group Security ist nach Massgabe der Direktive Sicherheit [3] für das Security Management im Konzern verantwortlich. Das Security Management umfasst insbesondere auch den Bereich der Information Security, der die Sicherstellung der Vertraulichkeit, Verfügbarkeit und Integrität von Daten zum Gegenstand hat.

Group Security unterstützt die Etablierung und Förderung der Datenkultur. Die Security Consultants beraten und unterstützen die Data Governance Managers bei der Einhaltung von Anforderungen im Bereich der Informationssicherheit.

7.8.2 Konzernrechtsdienst

Nach Massgabe der Direktive Recht [4] ist der Konzernrechtsdienst die zentrale Stelle im Bereich Recht der Swisscom. Er steht Führungskräften sowie Mitarbeitenden von Swisscom beratend und unterstützend zur Seite, damit diese ihre Arbeit erfolgreich ausführen und dabei ihre Verantwortung wahrnehmen können.

Der Konzernrechtsdienst berät und unterstützt die Unternehmensbereiche im Einzel- und Anwendungsfall bei der Einhaltung von Anforderungen im Bereich des Daten- und Geheimhaltungsschutzes.

7.8.3 VR-Internal Audit

Gemäss dem Ausführungsreglement Internal Audit [5] hat VR-Internal Audit die Aufgabe der unabhängigen und objektiven Prüfung und Beurteilung operativer Prozesse, des Internen Kontrollsystems sowie der Risikomanagement-, Steuerungs-, und Governance-Prozesse in allen Organisationseinheiten des Swisscom Konzern bezüglich Angemessenheit, Effizienz und Effektivität sowie bezüglich Vorschrifteneinhaltung.

VR-Internal Audit unterstützt DGO bei der Auditierung und Beurteilung der Einhaltung von Anforderungen bei Swisscom.

7.8.4 Group Compliance

Gemäss der Compliance-Policy [6] ist Group Compliance für die Konzeption und Umsetzung des zentralen Compliance-Systems im Swisscom-Konzern zuständig.

Group Compliance überwacht die Tätigkeiten von DGO im Rahmen des zentralen Compliance-Systems. Group Compliance bildet die Third Line of Defense.

7.8.5 Large Solution Data, Analytics and AI

Die Large Solution Data, Analytics & AI (DNA) speichert und administriert die Daten von Swisscom. Sie unterstützt die Linien mit Datenanalysen und Daten-Insights. Ihre Aufgaben umfassen unter anderem die Umsetzung einer unternehmensweiten Datenstrategie, die Optimierung und Automatisierung von internen Prozessen, die Entwicklung von neuen Produkten und Dienstleistungen auf der Basis von Daten und künstlicher Intelligenz und die Koordination von Investitionen und Akquisitionen.

DNA und DGO arbeiten bei der Entwicklung und Umsetzung der Datenkultur eng zusammen. DNA stellt insbesondere auch die Umsetzung von Massnahmen der Data Governance in ihrem Zuständigkeits- und Wirkungsbereich sicher.

7.8.6 Group Communications

Gemäss der Direktive Kommunikation & Corporate Responsibility [7] ist Group Communications and Corporate Responsibility für das Kommunikationsmanagement im Swisscom-Konzern zuständig. Diese Aufgabe beinhaltet insbesondere auch die Unterstützung im Bereich der Kommunikation.

Group Communications & Corporate Responsibility unterstützt DGO bei der Definition und Umsetzung von Kommunikationsinitiativen und -massnahmen zur Etablierung und Förderung der Datenkultur.

7.9 Kommunikation und Information

Mitarbeitende und Partner werden im Bereich des Daten- und gesetzlichen bzw. vertraglichen Geheimhaltungsschutzes über die Anforderungen und Massnahmen sowie die relevanten Zuständigkeiten informiert und soweit erforderlich geschult. Die Schulungen erfolgen rollenadäquat und sind verpflichtend (Push). Zusätzlich erfolgen Kommunikationsmassnahmen zur Etablierung und Förderung der Datenkultur als unverbindliche Angebote (Pull).

Die Konzernleitung, der VR-Ausschuss Revision und der Verwaltungsrat der Swisscom AG werden über die Etablierung und Förderung der Datenkultur bei Swisscom regelmässig, zweckmässig, stufengerecht und vollständig informiert.

Die Assurance-Funktionen Group Compliance, Risikomanagement und Internal Audit werden über wesentliche Compliance-Risiken regelmässig informiert.

7.10 Überwachung und Verbesserung

Die Angemessenheit und Wirksamkeit des DGS wird durch die Organisationseinheit Data Governance überprüft und von VR-Internal Audit (gemäss Integriertem Strategischen Prüfplan) periodisch auditiert. Erkannte Schwachstellen werden behoben.

Nach Umsetzung der Anordnungen und Massnahmen werden die Risiken mit Bezug auf deren Wirksamkeit für die Compliance-Berichterstattung erneut beurteilt.

Referenzierte Dokumente

[1] Direktive Data Governance

[2] Ausführungsreglement Internal Audit

[3] Direktive Sicherheit

[4] Direktive Recht

[5] Assurance Framework 4.0

[6] Compliance-Policy

[7] Direktive Kommunikation & Corporate Responsibility

* * * * * *