DATENSCHUTZSTELLE
FÜRSTENTUM LIECHTENSTEIN

Verfahrensbeschreibung für Datenschutzüberprüfungen

	Verfahrensbeschreibung von Datenschutzüberprüfungen
Dokument	DSS_Verfahrensbeschreibung_Datenschutzüberprüfungen.pdf
Version	1.0
vom	19. Juni 2020
Ersetzt Dokument	
Klassifizierung	öffentlich/public

Änderungskontrolle:

Version	Datum	Überarbeitung
1.0	19.06.2020	

Version: 19.06.2020, 14:31:00

Inhaltsverzeichnis

Einleitung und Rechtsrahmen

Die **Datenschutzstelle** (DSS) ist die einzige unabhängige staatliche Stelle (Aufsichtsbehörde) nach Art. 51 Datenschutz-Grundverordnung (DSGVO) und Art. 9 Abs. 1 Datenschutzgesetz (DSG) im Fürstentum Liechtenstein.[1] Als solche ist sie **zuständig für die Überwachung und Aufsicht über die von öffentlichen und nicht-öffentlichen Stellen** vorgenommenen Verarbeitungen personenbezogener Daten.[2]

Die DSS ist jedoch **nicht zuständig** für die Aufsicht über die von der Regierung im Rahmen ihrer Tätigkeit sowie die von den Gerichten im Rahmen ihrer justiziellen Tätigkeit vorgenommenen Verarbeitungen personenbezogener Daten.[3]

Aus den Bestimmungen der DSGVO und dem DSG ergibt sich für die DSS nicht nur die Zuständigkeit, sondern vielmehr eine **Verpflichtung zur Überwachung und Durchsetzung** des Datenschutzes.[4] Um dieser Verpflichtung nachzukommen, wurde die Aufsichtsbehörde durch den Gesetzgeber mit entsprechenden Befugnissen ausgestattet.[5] Diese Befugnisse der DSS erstrecken sich ebenso auf von öffentlichen oder nicht-öffentlichen Stellen erlangte personenbezogene Daten, über den Inhalt und die näheren Umstände des Brief-, Post und Fernmeldeverkehrs sowie personenbezogene Daten, die einem Amtsgeheimnis unterliegen.[6]

Die DSS unterscheidet Untersuchungen wie folgt:

1. Untersuchungen im Einzelfall aufgrund von Beschwerden oder Hinweisen;
2. Präventive oder anlasslose Untersuchungen in Form von Datenschutzüberprüfungen;
3. Untersuchungen auf Anfrage eines Verantwortlichen oder Auftragsverarbeiters;
4. Untersuchungen aufgrund eines gesetzlichen Auftrags;
5. Koordinierte gemeinsame Untersuchungen.

Untersuchungen im Einzelfall aufgrund von Beschwerden oder Hinweisen

Ist eine betroffene Person der Ansicht, die Verarbeitung ihrer personenbezogenen Daten durch eine bestimmte öffentliche oder nicht-öffentliche Stelle verstösst gegen die DSGVO oder das DSG, steht ihr das Recht zu, eine Beschwerde bei der DSS einzureichen.[7] Eine Beschwerde bei der DSS ist kostenlos[8] und kann über ein Online-Formular[9] eingereicht werden.

---

[1] Vgl. Art. 41 Richtlinie (EU) 2016/680 des europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates.
[2] Art. 51 Abs. 1 DSGVO iVm Art. 10 DSG.
[3] Art. 55 Abs. 3 DSGVO und Art. 10 Abs. 2 DSG.
[4] Art. 57 Abs. 1 Bst. a DSGVO und Art 15 Abs. 1 Bst. a DSG.
[5] Art. 58 DSGVO und 17 DSG.
[6] Art. 17 Abs. 3 DSG.
[7] Art. 77 DSGVO bzw. Art. 60 DSG.
[8] Gegen eine Verfügung der DSS können jedoch sämtliche beteiligten Parteien gemäss Art. 20 Abs. 1 DSG binnen vier Wochen ab Zustellung Beschwerde bei der Beschwerdekommission für Verwaltungsangelegenheiten erheben. Eine solche Prüfung durch die Beschwerdekommission für Verwaltungsangelegenheiten ist mit Kosten verbunden, welche entsprechend der massgebenden Bestimmungen des Gesetzes über die allgemeine Landesverwaltungspflege (LVG) sowohl dem Beschwerdegegner als auch dem Beschwerdeführer auferlegt werden können. Zur Klärung der Zulässigkeit dieses Umstands sind aktuell (Juni 2020) zwei Fälle beim EFTA-Gerichtshof hängig.
[9] https://www.datenschutzstelle.li/services-und-downloads/formulare#Beschwerdeformular.

Die betroffene Person hat des Weiteren das Recht auf einen wirksamen Rechtsbehelf, wenn die DSS die Beschwerde nicht bearbeitet oder nicht innerhalb von drei Monaten über den Fortgang oder das Ergebnis der Beschwerde informiert.[10]

Die DSS befasst sich aus diesem Grund mit jeder Beschwerde und wird den Gegenstand der Beschwerde in angemessenem Umfang untersuchen und die betroffene Person innerhalb einer angemessenen Frist über den Fortgang und das Ergebnis der Untersuchung unterrichten.

Präventive oder anlasslose Untersuchungen

Es ist der DSS jederzeit möglich, Untersuchungen über die Anwendung der DSGVO und des DSG von Amts wegen durchzuführen.[11] Der Aufgabenbereich der DSS wurde durch den Gesetzgeber bewusst weit gefasst, sodass präventive oder anlasslose Untersuchungen rechtlich zulässig und insbesondere zur wirksamen Überwachung der Anwendung und Durchsetzung der DSGVO auch geboten sind. Es ist somit nicht notwendig, dass etwa ein Anfangsverdacht, eine Beschwerde nach Art. 77 DSGVO, ein Hinweis, eine Meldung oder ein sonstiger wie auch immer gearteter Anlass vorliegt.

Im Sinne der Prävention führt die DSS somit regelmässig ohne konkreten Anlass Untersuchungen in Form von Datenschutzüberprüfungen (engl. *inspections* oder *audits*) durch. Es wird bei der Auswahl insbesondere auf das Risiko für die betroffenen Personen geachtet. Dazu wird insbesondere auf folgende Quellen und Kriterien abgestellt:

- Internetauftritt der datenverarbeitenden Stelle;
- Tätigkeitsberichte, Jahresberichte oder andere öffentlich zugängliche Informationen, die eine datenverarbeitende Stelle veröffentlicht hat;
- Vergangene Kontakte mit der jeweiligen Stelle, die ein wenig ausgeprägtes Verständnis für den Datenschutz erkennen liessen;
- Einführung neuartiger Datenverarbeitungen, wobei bestimmte öffentliche Bedenken dahingehend bestehen, dass die Privatsphäre gefährdet sein könnte;
- Umfang und die Art der zu verarbeitenden personenbezogenen Daten;
- Anzahl, Art sowie Inhalt von Beschwerden gegenüber einer bestimmten Kategorie datenverarbeitender Stellen;
- Ergebnisse vergangener Datenschutzüberprüfungen;
- Medienberichte.

Die Auswahl wird regelmässig mit weiteren öffentlichen und nicht-öffentlichen Stellen ergänzt, welche nach dem Zufallsprinzip ausgewählt werden. Dadurch wird sichergestellt, dass ebenso datenverarbeitende Stellen für eine Datenschutzüberprüfung ausgewählt werden, die sich bisher unauffällig gaben oder bei denen die Risiken für die betroffenen Personen auf den ersten Blick nicht immer erkennbar sind.

Untersuchungen auf Anfrage eines Verantwortlichen oder Auftragsverarbeiters

Ebenso ist es möglich und zulässig, dass sich eine öffentliche oder nicht-öffentliche Stelle freiwillig für eine Datenschutzüberprüfung bei der DSS meldet. In solchen Fällen entscheidet die DSS im Einzelfall, ob die Voraussetzungen für eine freiwillige Überprüfung der DSS gegeben sind.

[10] Art. 78 DSGVO.
[11] Art. 57 Abs. 1 Bst. h DSGVO bzw. Art. 15 Abs. 1 Bst. h DSG.

Untersuchungen aufgrund eines gesetzlichen Auftrags

Die oben erwähnte jährliche Auswahl der zu überprüfenden datenverarbeitenden Stellen wird mit jenen ergänzt, für welche die DSS einen gesetzlichen Auftrag zur Durchführung von regelmässigen Datenschutzüberprüfungen hat, wie z. B. aufgrund der Schengen-Mitgliedschaft Liechtensteins[12] oder im Zusammenhang mit der Vorratsdatenspeicherung[13].

Koordinierte gemeinsame Untersuchungen

Die EU/EWR-Aufsichtsbehörden führen in bestimmten Fällen gemeinsame Massnahmen einschliesslich gemeinsamer Untersuchungen und gemeinsamer Durchsetzungsmassnahmen durch.[14] Die DSS nimmt an solchen Untersuchungen teil, wenn eine gesetzliche Verpflichtung besteht oder es im Einzelfall geboten scheint.

Datenschutzüberprüfungen

Die DSS verfügt über die Befugnis, Untersuchungen in Form von Datenschutzüberprüfungen durchzuführen.[15] Ziel einer Datenschutzüberprüfung ist es, einen bei der überprüften Stelle **festgestellten Sachverhalt (Ist-Zustand) zu bewerten und insbesondere durch Anweisungen Datenverarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DSGVO bzw. dem DSG (Soll-Zustand) zu bringen**.

Datenschutzüberprüfungen und Untersuchungen im weitesten Sinn umfassen im Wesentlichen sechs Schritte, wobei der Ablauf nicht in allen Fällen streng chronologisch sein muss. Das Wiederholen von einzelnen oder mehreren Prüfschritten sowie Sprünge zwischen den Schritten sind jederzeit möglich. Diese sechs Schritte sind:

1. Kontaktaufnahme und Ankündigung;
2. Dokumentenprüfung;
3. *(optional)*;
4. Prüfbericht;
5. Wahrnehmung der Abhilfebefugnisse und Verfügung;
6. Anschlussprüfung (Follow-up).

Für alle Datenschutzüberprüfungen und Untersuchungen gilt für die DSS der Grundsatz, dass die Kontrolltätigkeit unter möglichster Schonung der Rechte der öffentlichen oder nicht-öffentlichen zu überprüfenden Stellen sowie Dritter auszuüben ist.[16]

Mitwirkungspflicht

Der Verantwortliche ist für die Einhaltung der Grundsätze der DSGVO und des DSG verantwortlich und muss deren Einhaltung auf Anfrage gegenüber der DSS nachweisen können („Rechenschaftspflicht“).[17] Bei Datenschutzüberprüfungen und Untersuchungen durch die DSS besteht für die öffentlichen oder nicht-öffentlichen Stellen, unabhängig ob

[12] Vgl. Art. 53 N-SIS-V iVm Art. 44 Abs. 2 VERORDNUNG (EG) Nr. 1987/2006 sowie Art. 60 Abs. 2 BESCHLUSS 2007/533/JI des Rates.
[13] Vgl. Art 52b KomG (Datenschutz und Kontrolle des Datenschutzes).
[14] Art. 62 DSGVO.
[15] Art. 58 Abs. 1 Bst. b DSGVO.
[16] Art. 17 Abs. 5 DSG.
[17] Art. 5 Abs. 2 DSGVO.

Verantwortlicher, Auftragsverarbeiter oder gegebenenfalls deren Vertreter, die Pflicht zur Zusammenarbeit.[18]

So haben die öffentlichen oder nicht-öffentlichen Stellen insbesondere alle Informationen, die für die Erfüllung der Aufgaben der DSS erforderlich sind, bereitzustellen. Im Fall nicht-öffentlicher Stellen kann die oder der Informationspflichtige die Information verweigern, wenn deren Bereitstellung sie oder ihn selbst oder Angehörige gemäss § 108 Abs. 1 der Strafprozessordnung der Gefahr strafgerichtlicher Verfolgung aussetzen würde.[19]

Die datenverarbeitenden Stellen sind unter anderem ebenso verpflichtet, der DSS sowie den von ihr mit der Überwachung der Einhaltung der Vorschriften über den Datenschutz beauftragten Personen Zugang zu den Grundstücken und Räumen, einschliesslich aller Datenverarbeitungsanlagen und -geräte, sowie zu allen personenbezogenen Daten und Informationen, die zur Erfüllung ihrer Aufgaben notwendig sind, zu gewähren. Die DSS hat dies jedoch vorgängig anzukündigen.[20]

Die Mitwirkungspflicht für Verantwortliche und Auftragsverarbeiter ist ebenso mit der Rechenschaftspflicht in Art. 5 Abs. 2 DSGVO dahingehend verankert, dass die Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten nachweisbar sein muss. Die Nichtmitwirkung bei Datenschutzüberprüfungen ist strafbewehrt.[21]

1. Kontaktaufnahme und Ankündigung

Eine erste Kontaktaufnahme erfolgt in der Regel mit einem **Anschreiben**, worin die zu prüfende Stelle über die bevorstehende Datenschutzüberprüfung oder Untersuchung durch die DSS informiert sowie über die Rechte und Pflichten aufgeklärt wird. Inhaltlich wird das Schreiben in vielen Fällen bereits den geplanten Prüfungsumfang enthalten. Zudem wird die angeschriebene öffentliche oder nicht-öffentliche Stelle meist mit diesem Anschreiben bereits aufgefordert, zu spezifischen Fragen – vorwiegend in Form eines Fragenkatalogs – Stellung zum geprüften Gegenstand zu nehmen sowie entsprechende Informationen und Dokumente, die für die Prüfung erforderlich sind, bereit bzw. zur Verfügung zu stellen.[22]

Wurde eine Datenschutzbeauftragte oder ein Datenschutzbeauftragter (DSB) benannt und der DSS mitgeteilt,[23] ergeht das Anschreiben an die bei der DSS gemeldete Person.[24] Die zu prüfende Stelle wird im Anschreiben ersucht, eine Person als **Koordinations- bzw. Kontaktperson** gegenüber der DSS zu benennen. In der Regel wird diese Kontaktperson die oder der DSB selbst sein. Jedenfalls sollte diese Person während der Datenschutzüberprüfung oder Untersuchung gut erreichbar sein und ebenso die entsprechenden Kompetenzen besitzen, die allfällig von der DSS angeforderte Dokumentation sowie Unterlagen innert Frist zu besorgen oder die zu interviewenden Personen für kurze Zeit aus dem Regelbetrieb herauszulösen.

[18] Art. 31 DSGVO.
[19] Art. 17 Abs. 4 Bst. b DSG.
[20] Art. 17 Abs. 4 Bst. a DSG.
[21] Art. 83 Abs. 4 Bst. a DSGVO oder Art. 83 Abs. 5 Bst. a DSGVO.
[22] Insbesondere das Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 Abs. 4 DSGVO.
[23] Vgl. Art. 37 Abs. 7 DSGVO.
[24] Vgl. Art. 39 Abs. 1 Bst. e DSGVO.

Abhängig von der Art einer Datenschutzüberprüfung oder Untersuchung kann es zweckmässig und geboten sein, vor der Festlegung des konkreten Prüfungsumfangs und dem Versand spezifischer Fragen oder einer Aufforderung zur Stellungnahme eine der Prüfung **vorgelagerte Besprechung** mit sämtlichen beteiligten Personen von Seiten der zu prüfenden Stelle (z. B. Geschäftsleitung, DSB) sowie der DSS (z. B. Leitung, Audit-Team) durchzuführen. Diese Besprechung soll insbesondere der Erläuterung des Verfahrens und Klärung organisatorischer Fragen, der Abgrenzung und Festlegung des konkreten Prüfungsumfangs sowie der Absprache betreffend die weiteren Termine und Verfügbarkeiten dienen. Eine solche Besprechung ist jedoch nicht in allen Fällen zwingend notwendig. Sie wird daher vor allem bei umfangreicheren Untersuchungen oder komplizierteren Sachverhalten durchgeführt.

Sollten es **besondere Umstände oder Gefahr in Verzug** erfordern, ist eine Datenschutzüberprüfung oder Untersuchung nach vorgängiger Verständigung – wobei hier *kein* Erfordernis der Schriftlichkeit besteht – bei der zu prüfenden Stelle jederzeit möglich. Diese Vorgehensweise ist jedoch ausschliesslich auf Ausnahmesituationen anzuwenden. In dringenden Fällen bei aktueller und fortdauernder Verletzung der Privatsphäre betroffener Personen mit einer gewissen Schwere kann ein sofortiges Einschreiten der DSS notwendig sein und ist in diesen Fällen gerechtfertigt.

Ob bei einer Beschwerde oder Meldung die betroffene Person gegenüber einer zu prüfenden öffentlichen oder nicht-öffentlichen Stelle genannt wird, ist im Einzelfall nach Anhörung des Beschwerdeführers zu entscheiden.[25] Im Sinne der Akzeptanz und zur Stärkung des allgemeinen Prüfklimas scheint die Nennung der Umstände und konkreten Gründe einer Datenschutzüberprüfung oder Untersuchung empfehlenswert.

2. Dokumentenprüfung

Die DSS verfügt über sämtliche Untersuchungsbefugnisse, die es ihr gestatten, eine zu prüfende öffentliche oder nicht-öffentliche Stelle anzuweisen, alle Informationen bereitzustellen, die für die Erfüllung ihrer Aufgaben erforderlich sind.[26] In einem ersten Schritt wird die DSS von der zu überprüfenden Stelle entsprechende Informationen und Stellungnahmen in Form eines Fragenkatalogs einholen. Zusätzlich zur Beantwortung der Fragen sind der DSS auf Anfrage regelmässig folgende Informationen und Unterlagen in elektronischer Form oder auf Papier zur Verfügung bzw. bereitzustellen:

- Verzeichnis der Verarbeitungstätigkeiten (Art. 30 Abs. 4 DSGVO);
- Informationen an die betroffenen Personen (Art. 13 und 14 DSGVO);
- Muster von Einwilligungserklärungen (Art. 7 DSGVO);
- Informationen zu Datenschutzschulungen der Mitarbeitenden;
- Verträge mit Auftragsverarbeitern (Art. 28 Abs. 3 DSGVO) oder andere aktuelle Verträge mit allfälligen Dienstleistungserbringern, die mit personenbezogenen Daten in Berührung kommen (z. B. Hard- und Softwarelieferanten, Application Service Provider), wobei die jeweiligen Datenschutzbestimmungen hervorzuheben sind;
- Dokumentation von Datenschutzverletzungen (Art. 33 Abs. 5 DSGVO);
- Datenschutz-Folgenabschätzungen (Art. 35 DSGVO).

[25] Vgl. dazu https://eftacourt.int/cases/case-e-1119/ und https://eftacourt.int/cases/case-e-12-19/.
[26] Art. 58 Abs. 1 DSGVO und Art. 17 Abs. 4 Bst. b DSG.

Zum Zwecke des Nachweises der Einhaltung der DSGVO und des DSG sowie zur Beurteilung vor allem der Wirksamkeit der technischen und organisatorischen Massnahmen wird die DSS regelmässig folgende weitere Informationen von der zu prüfenden Stelle verlangen:

- Organigramm der datenverarbeitenden Organisationseinheiten;
- Datenschutzpolitik, IT-Sicherheitsstrategie und Notfallplanung;
- Revisions- oder Prüfberichte anderer Stellen, insbesondere im Zusammenhang mit dem Prüfungsumfang bezüglich der Informationstechnologie im Allgemeinen;
- Basisdokumentation der IT-Infrastruktur, wie insbesondere die verwendete Soft- und Hardware;
- Konzept der Zugriffsberechtigungen, insbesondere eine Darstellung der Rechte von Administratoren, externen Mitarbeitern und Dienstleistenden oder anderen (externen) Stellen;
- Weisungen an die Benutzerinnen und Benutzer für die Verwendung der Informatikmittel;
- Geheimhaltungserklärungen oder andere sachverhaltsrelevante Weisungen;
- Regelungen betreffend die Aufbewahrungsdauer und Löschung personenbezogener Daten (Löschkonzept);

Der Umfang und Detaillierungsgrad der zur Verfügung zu stellenden Dokumentation hängt insbesondere vom Prüfungsumfang und Zweck der konkreten Untersuchung bzw. Datenschutzüberprüfung ab. Die zur Verfügung gestellte Dokumentation sollte die mit dem Anschreiben übermittelten Fragen ausreichend beantworten und die in einer allfälligen Stellungnahme ausgeführten Erläuterungen der überprüften Stelle belegen können.

HINWEIS: Die Dokumentation darf nicht via E-Mail oder andere unsichere Kommunikationskanäle an die DSS gesendet werden. Für die sichere elektronische Übermittlung von Dokumenten/Dateien steht den geprüften Stellen auf der Internetseite der DSS ein entsprechendes Kontaktformular zur Verfügung.[27]

Während der Dokumentenprüfung kann es sein, dass die DSS Informationen nachfordert oder zwecks Verständnisfragen zu den übermittelten Dokumenten telefonische Interviews mit bestimmten Personen der zu prüfenden Stelle führt.

Im Ergebnis der Dokumentenprüfung entscheidet die DSS, ob für die vollständige Beurteilung eines Sachverhalts oder die Prüfung der Wirksamkeit bestimmter technischer und organisatorischer Massnahmen eine Prüfung vor Ort notwendig ist. Falls eine solche aufgrund der vorgelegten Informationen und Unterlagen aus Sicht der DSS notwendig scheint, wird die zu prüfende Stelle über diesen Schritt informiert. Andernfalls wird die Untersuchung bzw. die Datenschutzüberprüfung mit dem Prüfbericht (Abschnitt 4, S. 10) fortgesetzt.

[27] https://www.datenschutzstelle.li/services-und-downloads/formulare#secfiletransfer.

3. Prüfung vor Ort

Ergibt sich aufgrund der konkreten Umstände oder des Sachverhalts, dass eine Prüfung vor Ort zur Beurteilung der Wirksamkeit implementierter technischer und organisatorischer Massnahmen oder zur Prüfung anderer Aspekte der Datenverarbeitung notwendig ist, wird die DSS die zu prüfende Stelle darüber informieren und die geplante Prüfung vor Ort vorgängig ankündigen.

Die öffentlichen sowie nicht-öffentlichen Stellen sind verpflichtet, der DSS und gegebenenfalls den von ihr mit der Überwachung der Einhaltung der Vorschriften über den Datenschutz beauftragten Personen Zugang zu den Grundstücken und Räumen, einschliesslich aller Datenverarbeitungsanlagen und -geräte, sowie zu allen personenbezogenen Daten und Informationen, die zur Erfüllung ihrer Aufgaben notwendig sind, zu gewähren. Die DSS hat dies jedoch vorgängig anzukündigen.[28]

Die Zeit für die Prüfung vor Ort wird jedoch knapp bemessen sein, insbesondere um die Ressourcen der geprüften Stelle zu schonen sowie überflüssige Kosten und übermässige Unannehmlichkeiten für sämtliche Beteiligten zu vermeiden.[29] Die Prüfungen vor Ort finden in der Regel während der Bürozeiten statt. Für einen ausserhalb der Bürozeiten stattfindenden Zutritt – ebenso die Bereitstellung von Informationen – bleibt nur dann Raum, wenn die Aufsichtstätigkeit der DSS ansonsten geradezu verunmöglicht würde. Die Prüfungen vor Ort dauern in der Regel einen halben Tag. Sie kann jedoch ausnahmsweise bei umfangreicheren Prüfungen, z. B. bei der Verteilung einer Datenverarbeitung auf mehrere (Unternehmens-)Standorte, auf mehrere Tage ausgedehnt werden. Damit die Prüfung vor Ort so rasch und schonend wie möglich durchgeführt werden kann, wird die zu prüfende Stelle angehalten, die Verfügbarkeit der Personen sicherzustellen, die entsprechende Ausführungen und Erläuterungen zu Datenverarbeitungsvorgängen geben können.

Begonnen wird – wenn aufgrund der Umstände nicht anderweitig vereinbart – mit einer Eröffnungsbesprechung mit der Geschäftsführung oder anderen Entscheidungsträgern der zu prüfenden öffentlichen oder nicht-öffentlichen Stelle sowie der gegenüber der DSS genannten Ansprechperson[30] und falls nötig mit weiteren Mitarbeitenden. Dabei informiert das Audit-Team der DSS über die bereits erfolgten Schritte (Auswertung der zur Verfügung gestellten Unterlagen sowie den Status der geprüften Dokumentation) und den weiteren Ablauf. Ebenso bietet diese Sitzung sämtlichen Beteiligten die Möglichkeit, das bis zu diesem Zeitpunkt Geschehene zu erörtern, den Zeitplan für die weitere Prüfung vor Ort festzulegen und allfällige Fragen zu beantworten.

Nach der Eröffnungsbesprechung erfolgen die Klärung der offenen Punkte sowie das Einholen von weiteren Informationen vor allem durch Interviews entsprechender Mitarbeiterinnen und Mitarbeiter der zu prüfenden Stelle.

Zur Beurteilung der Wirksamkeit insbesondere von organisatorischen Massnahmen, wie etwa die Umsetzung von Zutrittskontrollen usw., ist es durchaus notwendig, bestimmte Abläufe in der Praxis zu begutachten. Von grosser Bedeutung ist ebenso die stichprobenartige Überprüfung der Verarbeitung konkreter Einzelfälle. Eine begleitende Begutachtung

[28] Art. 58 Abs. 1 Bst. f DSGVO iVm Art. 17 Abs. 4 Bst. a DSG.
[29] Vgl. Art. 17 Abs. 5 DSG und ErwG. 129 DSGVO.
[30] In der Regel wird diese Kontaktperson die oder der Datenschutzbeauftragte sein.

des Prozesses in verschiedensten Räumlichkeiten der zu prüfenden Stelle ist in vielen Fällen daher unumgänglich.

Der allfällige Einsatz von Software sowie jede andere Interaktion mit der zu prüfenden IT-Infrastruktur – wenn dies im Einzelfall notwendig sein sollte – erfolgt ausschliesslich unter Einbeziehung der zuständigen (externen/internen) Fachpersonen der zu prüfenden Stelle.

Die DSS behält sich vor, bei Feststellung oder Beobachtung aktueller Datenschutzverletzungen den Prüfungsumfang jederzeit zu erweitern. In diesem Falle wird die DSS die zu prüfenden Stelle darüber informieren.

Die DSS kann, wenn es notwendig scheint, externe Sachverständige zur Prüfung bestimmter Sachverhalte beiziehen. Die zu prüfende Stelle wird über diese Entscheidung frühzeitig in Kenntnis gesetzt.

Am Ende der Prüfung vor Ort sollte eine Abschlussbesprechung mit den wichtigsten Personen – im besten Fall mit jenen aus der Eröffnungsbesprechung – stattfinden. Das Audit-Team der DSS wird die Feststellungen und Wahrnehmungen zusammenfassen, wobei in dieser Phase keinerlei Bewertungen einzelner Sachverhalte vorgenommen werden. Abschliessend wird die DSS über die weiteren Schritte und das weitere Verfahren informieren. Dabei werden insbesondere die Termine und Fristen für die nächsten Schritte erläutert und – wenn immer möglich und zulässig – im gegenseitigen Einvernehmen abgestimmt.

4. Prüfbericht

Die DSS erarbeitet grundsätzlich für jede Datenschutzüberprüfung und Untersuchung einen Prüfbericht. Dieser enthält insbesondere:

1. Audit-Team der DSS sowie beteiligte Personen der geprüften Stelle;
2. Prüfungszeitpunkt und -umfang sowie den Prüfungsgegenstand;
3. Zusammenfassung des Ergebnisses betreffend die einzelnen Prüfpunkte;
4. Darstellungen allfälliger Abweichungen (Soll-Ist-Vergleich) in Bezug auf die einzelnen Prüfpunkte (Art, Schwere, Dauer usw.) **zum Zeitpunkt der Datenschutzüberprüfung oder Untersuchung**;
5. Rechtliche sowie technische Bewertungen zu den einzelnen Abweichungen;
6. Darstellung allfälliger, im Zuge oder im Anschluss der bzw. an die Datenschutzüberprüfung oder Untersuchung getroffener Massnahmen durch die geprüfte Stelle.

Der Prüfbericht fasst die Ergebnisse der Prüfung zusammen und enthält keine Empfehlungen oder Anweisungen nach Art. 58 Abs. 2 DSGVO. Diese werden gegebenenfalls im Anschluss an die Datenschutzüberprüfung oder Untersuchung gestützt auf das jeweilige Ergebnis mit einer eigenen rechtsmittelfähigen Verfügung der geprüften Stelle zugestellt.

4.1 Bewertungskriterien

Im Rahmen der Bewertung wird beurteilt, ob und mit welchem Grad die einzelnen Verarbeitungstätigkeiten einer gesetzeskonformen Umsetzung der datenschutzrechtlichen und -technischen Bestimmungen entsprechen. Der **Umsetzungsgrad** ist dabei auf Grundlage folgender Kriterien zu bestimmen:

Stufe	**Bezeichnung**	
0	Nicht vorhanden	Die Datenschutzanforderungen und Grundsätze werden nicht berücksichtigt oder sind nicht bekannt. Es sind keinerlei Verfahren, bspw. zur Berücksichtigung der Betroffenenrechte, vorhanden und es wurden ebenso noch keine technischen wie organisatorischen (Sicherheits-)Massnahmen initiiert oder der Bedarf wurde noch nicht erkannt.
1	Initial	Die Datenschutzanforderungen und Grundsätze sind bekannt. Verfahren und (Sicherheits-)Massnahmen sind lediglich geplant oder in wenigen Teilbereichen umgesetzt. Es kommen teilweise informelle Verfahren, bspw. zur Berücksichtigung der Betroffenenrechte, zum Einsatz. Diese sind nicht standardisiert, nicht wiederholbar und nicht allen datenverarbeitenden oder für die Datenverarbeitung verantwortlichen Personen bekannt. Ansätze für strukturierte Verfahren sind zwar vorhanden, Probleme werden jedoch ad hoc und reaktiv, individuell oder situationsbezogen gelöst.
2	Wiederholbar	Das Bewusstsein für den Datenschutz ist auf allen Unternehmensstufen vorhanden. Strukturierte und wiederholbare Prozesse wurden so entwickelt, dass gleichartige Verfahren von unterschiedlichen Personen angewandt werden können, die dieselbe Aufgabe wahrnehmen. Es besteht kein formales Training und die Verantwortung ist den Einzelpersonen überlassen. Es wird auf das Wissen der Einzelpersonen vertraut. Die Prozesse sowie technischen und organisatorischen Massnahmen sind mit wenigen Lücken dokumentiert und den datenverarbeitenden sowie verantwortlichen Personen bekannt. Die Umsetzung betrifft Teilbereiche.
3	Definiert	Die Datenschutzanforderungen und Grundsätze werden auf allen Unternehmensstufen „gelebt“. Verfahren und Massnahmen wurden standardisiert, sind dokumentiert und durch Trainings kommuniziert. Die Einhaltung ist jedoch den Einzelpersonen überlassen und die Erkennung von Abweichungen ist unwahrscheinlich. Die Verfahren sind nicht ausgereift und sind ein formalisiertes Abbild bestehender Praktiken.
4	Vollständig umgesetzt	Die Datenschutzanforderungen und Grundsätze werden auf allen Unternehmensstufen „gelebt“. Der datenverarbeitenden Stelle ist es möglich, die Einhaltung von Verfahren und Massnahmen zu überwachen sowie Aktionen dort zu ergreifen, wo Prozesse nicht wirksam funktionieren. Die bestehenden Verfahren und Massnahmen werden laufend verbessert und folgen Good Practices.

5	Optimiert	Die Verfahren und (Sicherheits-)Massnahmen wurden, basierend auf laufender Verbesserung und Vergleichen mit anderen Unternehmen, auf ein Best-Practice-Niveau verbessert. Die Massnahmen werden weiter laufend optimiert.

4.2 Gelegenheit zur Stellungnahme

Der zusammengefasste Sachverhalt sowie allfälligen Feststellungen vor Ort werden durch die DSS der geprüften öffentlichen oder nicht-öffentlichen Stelle zur Stellungnahme zugestellt. Dadurch bekommt sie die Gelegenheit, unvollständige oder von der DSS missverstandene Sachverhalte betreffend die Befundaufnahme (Ist-Zustand) zu ergänzen oder klarzustellen sowie Missverständnisse aller Art aufzulösen. Die Stellungnahme der überprüften Stelle kann ferner eine Darstellung jener Massnahmen enthalten, die aufgrund der Datenschutzüberprüfung oder Untersuchung der DSS durch die geprüfte Stelle zwischenzeitlich getroffen worden sind.

Gegen den Prüfbericht selbst sind keine Rechtsmittel zulässig, da dieser ausschliesslich den festgestellten Sachverhalt sowie allfällige Abweichungen (engl. *findings*) in Bezug auf die verschiedenen Prüfpunkte **zum Zeitpunkt der Datenschutzüberprüfung oder Untersuchung** festhält. Allfällig notwendiger Handlungsbedarf der datenverarbeitenden Stelle werden dieser in Form von Anweisungen, Anordnungen, Beschränkungen oder Verboten gemäss Art. 58 Abs. 2 DSGVO mittels rechtsmittelfähiger Verfügung zugestellt.

5. Wahrnehmung der Abhilfebefugnisse und Verfügung

Die DSS wird im Anschluss an die Fertigstellung des Prüfberichts eine entsprechende Verfügung an die der DSS gegenüber bezeichnete Kontaktperson zustellen. Diese Verfügung enthält unter anderem:

1. Präambel;
2. Spruch;
3. Sachverhalt/Feststellungen;
4. Rechtliche Beurteilung;
5. Rechtsmittelbelehrung;
6. Prüfbericht als Beilage *(optional)*.

Gemäss Art. 58 Abs. 2 DSGVO bedient sich die DSS entsprechender Abhilfebefugnisse, um bei Bedarf die datenschutzkonforme Datenverarbeitung bei der überprüften öffentlichen oder nicht-öffentlichen Stelle (wieder-)herzustellen.

5.1 Abhilfebefugnisse

Art. 58 Abs. 1 Bst. d DSGVO („Hinweis“): Die DSS kann sich dieser *Untersuchungsbefugnis* bedienen, um die überprüfte öffentliche oder nicht-öffentliche Stelle auf einen vermeintlichen Verstoss gegen die DSGVO hinzuweisen. Diese Befugnis dient vor allem der Prävention und soll der datenverarbeitenden Stelle die Möglichkeit geben, eine geplante Verarbeitungstätigkeit anders auszugestalten oder eine bereits laufende zeitnah anzupassen.

Art. 58 Abs. 2 Bst. a DSGVO („Warnung“): Mit der gegenständlichen Befugnis kann die DSS die überprüfte datenverarbeitende Stelle dahingehend warnen, dass ein beabsichtigter Verarbeitungsvorgang voraussichtlich gegen die DSGVO oder gegen im DSG enthaltene und andere auf die jeweilige Datenverarbeitung anzuwendende Vorschriften über den Datenschutz verstossen wird.[31] Ein wesentliches Kriterium dabei ist jeweils, dass es im konkreten Fall noch zu keiner Verarbeitung personenbezogener Daten gekommen ist.[32]

Art. 58 Abs. 2 Bst. b DSGVO („Verwarnung“): Die DSS kann die überprüfte datenverarbeitende Stelle verwarnen, wenn diese mit bestimmten Verarbeitungsvorgängen gegen die DSGVO verstösst oder verstossen hat. In Abgrenzung zur „Warnung“ nach Art. 58 Abs. 2 Bst. a DSGVO hat gegenständlich bereits eine Datenverarbeitung stattgefunden, die nicht den Vorgaben der DSGVO entsprochen hat. Die DSS wird insbesondere bei erstmaligen Verstössen von Abhilfebefugnis der Verwarnung Gebrauch machen.

Art. 58 Abs. 2 Bst. c DSGVO („Anweisung“): Um betroffene Personen bei der Durchsetzung ihrer Rechte nach der DSGVO[33] zu unterstützen, kann die DSS die verarbeitende Stelle anweisen, den Anträgen von Betroffenen zu entsprechen.

Art. 58 Abs. 2 Bst. d DSGVO („Anweisung“): Die DSS kann die überprüfte datenverarbeitende Stelle anweisen, Verarbeitungsvorgänge auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DSGVO zu bringen. Die DSS hat somit die Befugnis, anzuweisen, wie bestimmte Verarbeitungsvorgänge konkret – in einer bestimmten Weise – in Einklang mit der DSGVO zu bringen sind. Dies kann rechtliche, technische als auch organisatorische Bestimmungen der DSGVO betreffen.

Art. 58 Abs. 2 Bst. e DSGVO („Anweisung“): Ebenso kann die DSS den Verantwortlichen anweisen, die von einer Verletzung des Schutzes personenbezogener Daten betroffenen Personen entsprechend zu benachrichtigen.[34]

Art. 58 Abs. 2 Bst. f DSGVO („Beschränkung“ oder „Verbot“): Die DSS kann eine vorübergehende oder endgültige Beschränkung der Verarbeitung, einschliesslich eines Verbots, verhängen. Dabei handelt es sich um eine sehr weitreichende Massnahme. Die Möglichkeiten der Beschränkung oder des Verbots beziehen sich dabei auf alle von der DSS überprüften Verarbeitungsvorgänge, unabhängig davon, ob die Verarbeitung durch den Verantwortlichen selbst oder durch einen Auftragsverarbeiter geschieht.

Art. 58 Abs. 2 Bst. g DSGVO („Anordnung“): Die DSS kann die Berichtigung[35] oder Löschung[36] oder die Einschränkung der Verarbeitung[37] von personenbezogenen Daten sowie die Unterrichtung der Empfänger, denen diese personenbezogenen Daten gemäss Art. 17 Abs. 2 und Art. 19 DSGVO offengelegt wurden, gegenüber einem Verantwortlichen anordnen.

---

[31] Art. 17 Abs. 2 letzter Satz DSG.
[32] Vgl. Art. 4 Ziff. 2 DSGVO bzw. Art. 46 Bst. b DSG.
[33] Recht auf Information (Art. 13 und 14 DSGVO), Recht auf Auskunft (Art. 15 DSGVO), Recht auf Berichtigung (Art. 16 DSGVO), Recht auf Löschung bzw. Recht auf „Vergessenwerden“ (Art. 17 DSGVO), Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO), Recht auf Datenübertragbarkeit (Art. 20 DSGVO), Recht auf Widerspruch (Art. 21 DSGVO), Recht, nicht einer ausschliesslich auf einer automatisierten Verarbeitung – einschliesslich Profiling – beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt (Art. 22 DSGVO).
[34] Vgl. Art. 34 Abs. 4 DSGVO.
[35] Art. 16 DSGVO.
[36] Art. 17 DSGVO.
[37] Art. 18 DSGVO.

Art. 58 Abs. 2 Bst. h DSGVO („Anweisung“): Die DSS kann eine Zertifizierung widerrufen oder eine Zertifizierungsstelle anweisen, eine gemäss Artikel 42 und 43 DSGVO erteilte Zertifizierung zu widerrufen. Ebenso kann die DSS eine Zertifizierungsstelle anweisen, keine Zertifizierung zu erteilen, wenn die Voraussetzungen für die Zertifizierung nicht oder nicht mehr erfüllt werden.

Art. 58 Abs. 2 Bst. j DSGVO („Anordnung“): Die DSS kann ebenso die Aussetzung der Übermittlung von Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation anordnen.

Zudem kann die DSS gemäss **Art. 58 Abs. 2 Bst. i DSGVO** eine Geldbusse gemäss Art. 83 DSGVO verhängen. Dies zusätzlich zu den oder anstelle der in diesem Kapitel erwähnten Abhilfemassnahmen, je nach den Umständen des Einzelfalls. („Geldbusse“)

Welche Abhilfebefugnisse auszusprechen sind und welche Dringlichkeit diese haben, hängt im Wesentlichen von dem zu Grunde liegenden Sachverhalt und dessen datenschutzrechtlicher Relevanz im Gesamtgefüge ab.

5.2 Gelegenheit zur Stellungnahme

Mit Art. 17 Abs. 1 DSG wird sichergestellt, dass vor Ausübung bestimmter Befugnisse[38] durch die DSS, der jeweils für die überprüfte Stelle zuständigen Aufsichtsbehörde[39] die festgestellten Verstösse gegen die Vorschriften des Datenschutzes mitgeteilt werden und dadurch die Aufsichtsbehörde unter Setzung einer angemessenen Frist die Gelegenheit zu einer Stellungnahme erhält. Durch diese vorgängige Mitteilung der DSS soll insbesondere gewährleistet werden, dass die jeweils für die geprüfte Stelle zuständige Aufsichtsbehörde Kenntnis vom Verstoss erhält und vor der Ausübung weitergehender Befugnisse durch die DSS rechtliches Gehör findet. Die Gefahr divergierender Anweisungen zwischen Datenschutzaufsicht und den zuständigen Aufsichtsbehörden soll hierdurch reduziert werden. Die Bestimmung nimmt dabei konkret die Warnung nach Art. 58 Abs. 2 Bst. a DSGVO als auch die Anweisung im Zusammenhang mit Zertifizierungen nach Art. 58 Abs. 2 Bst. h DSGVO aus, da diese auf ein allenfalls vor einer anderen Aufsichtsbehörde laufendes Verfahren keinen Einfluss haben.

Von der Einräumung der Gelegenheit zur Stellungnahme kann die DSS absehen, wenn eine sofortige Entscheidung wegen Gefahr im Verzug oder im öffentlichen Interesse notwendig erscheint oder ihr ein zwingendes öffentliches Interesse entgegensteht. Die Stellungnahme der zuständigen Aufsichtsbehörde soll auch eine Darstellung der Massnahmen enthalten, die aufgrund der Mitteilung der DSS getroffen worden sind.[40]

5.3 Besonderheiten ausserhalb des Anwendungsbereichs der DSGVO

Stellt die DSS bei Datenverarbeitungen durch öffentliche oder nicht-öffentliche Stellen zu Zwecken **ausserhalb des Anwendungsbereichs der DSGVO** Verstösse gegen die Vorschriften des DSG oder gegen andere Vorschriften über den Datenschutz oder sonstige Mängel bei der Verarbeitung oder Nutzung personenbezogener Daten fest, so beanstandet sie dies gegenüber dem Verantwortlichen.

---

[38] Art. 58 Abs. 2 Bst. b bis g, i und j DSGVO.
[39] Zum Beispiel die Finanzmarktaufsicht Liechtenstein (FMA) oder das Amt für Kommunikation (AK).
[40] Art. 17 Abs. 1 DSG.

Im Fall einer öffentlichen Stelle informiert die DSS zusätzlich die Regierung über die Beanstandung. Sie gibt dem Verantwortlichen, im Falle einer öffentlichen Stelle zusätzlich der Regierung, Gelegenheit zu einer Stellungnahme innerhalb einer von der DSS zu bestimmenden angemessenen Frist. Die DSS kann von einer Beanstandung absehen oder auf eine Stellungnahme verzichten, insbesondere wenn es sich um unerhebliche oder inzwischen beseitigte Mängel handelt.[41]

Die Stellungnahme soll auch eine Darstellung jener Massnahmen enthalten, die aufgrund der Beanstandung der DSS durch die geprüfte Stelle zwischenzeitlich getroffen worden sind.

6. Anschlussprüfung (Follow-up)

Die geprüfte öffentliche oder nicht-öffentliche Stelle informiert die DSS nach Aufforderung über die – basierend auf der Verfügung – zwischenzeitlich getroffenen Massnahmen und Tätigkeiten innert angemessener Frist.

Die DSS behält sich vor, die Umsetzung der erforderlichen Massnahmen in einer Nachkontrolle zu überprüfen. Die Entscheidung darüber, ob eine Anschlussprüfung vor Ort stattfindet, wird der geprüften Stelle nach Sichtung allfälliger Unterlagen zum Nachweis der umzusetzenden Massnahmen sowie allfälliger weiterer Dokumentation mitgeteilt.

Sämtliche Folgeaktivitäten der DSS konzentrieren sich in erster Linie auf jene Bereiche, in welchen die Abweichungen festgestellt wurden und die grössten Risiken für die betroffenen Personen bestehen.

[41] Art. 17 Abs. 2 DSG.

Anhänge

Häufig gestellte Fragen

Wie viel Zeit nimmt eine Untersuchung bzw. Datenschutzüberprüfung in Anspruch?

Dies hängt sehr stark vom zu prüfenden Sachverhalt ab. Vom ersten Anschreiben der DSS bis zur finalen Verfügung an die geprüft Stelle vergehen nicht selten mehrere Monate. Dies liegt vor allem an den grosszügigen Fristen, welche die DSS den geprüften Stellen regelmässig für die Beibringung von Informationen, Dokumenten und Stellungnahmen einräumt. Sollten es der Sachverhalt zulassen oder besondere Umstände oder Gefahr in Verzug erfordern, kann eine Untersuchung wesentlich schneller durchgeführt und abgeschlossen werden.

Wie viel wird es kosten?

Für die überprüfte öffentliche oder nicht-öffentliche Stelle fallen für die Untersuchung seitens der DSS keine Kosten an. Bedient sich eine datenverarbeitende Stelle beispielsweise einer externen Stelle oder Experten, sind die dabei entstehenden Kosten durch die geprüfte Stelle selbst zu tragen.

Muss eine öffentliche oder nicht-öffentliche Stelle bei der Prüfung mitwirken?

Ja, es besteht eine Mitwirkungspflicht für die geprüfte Stelle. Details dazu siehe Abschnitt Mitwirkungspflicht ab S. 5.

Wie können der DSS sicher Dokumente übermittelt werden?

Für die sichere elektronische Übermittlung von Dokumenten/Dateien steht den geprüften Stellen auf der Internetseite der DSS ein entsprechendes Kontaktformular zur Verfügung. (https://www.datenschutzstelle.li/services-und-downloads/formulare#secfiletransfer)

Wird der Schlussbericht oder das Ergebnis der Prüfung veröffentlicht?

Die DSS veröffentlich jährlich in ihrem Tätigkeitsbericht zusammengefasst die Ergebnisse der Datenschutzüberprüfungen und Untersuchungen.