Datenschutzweisung für Mitarbeitende

Hotel Lenkerhof AG

Inhaltsverzeichnis

1. Zweck und Grundlagen 3
2. Geltungsbereich 3
3. Gegenstand 3
4. Begriffe 3
5. Grundsätze für die Bearbeitung von Personendaten 4
6. Besondere Bearbeitungstätigkeiten 8
7. Verzeichnis über die Bearbeitungstätigkeiten 10
8. Informationspflichten bei der Erhebung von Personendaten direkt bei der betroffenen Person 10
9. Informationspflichten bei der indirekten Erhebung von Personendaten 12
10. Rechte der betroffenen Personen 12
11. Übermittlung Personendaten an Dritte 17
12. Technische und organisatorische Massnahmen 17
13. Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen 18
14. Datenschutz-Folgenabschätzung 18
15. Meldung von Verletzungen der Datensicherheit 18
16. Verantwortlichkeiten 19
17. Sanktionen 20
18. Schlussbestimmungen 20

1. Zweck und Grundlagen

Diese Datenschutzweisung enthält Vorschriften zum Schutz von Personendaten, die für die Hotel Lenkerhof AG gelten. Die Weisung vermittelt den Mitarbeitenden die wichtigsten Grundlagen des Datenschutzes und ermöglicht ihnen, zusammen mit anderen Massnahmen und Dokumenten, ihre Tätigkeit im Einklang mit den anwendbaren datenschutzrechtlichen Vorgaben auszuüben.

Da das Unternehmen Hotellerie bezogene Dienstleistungen sowie gegebenenfalls weitere Dienstleistungen und Waren anbietet und in diesem Zusammenhang Personendaten bearbeitet, ergibt sich, dass die schweizerischen Datenschutzgesetze und gegebenenfalls auch weitere datenschutzrechtliche Vorgaben (z.B. die europäischen) für das Unternehmen relevant sind.

2. Geltungsbereich

Diese Datenschutzweisung gilt für alle Mitarbeitenden des Unternehmens, die Personendaten bearbeiten. Die Mitarbeitenden werden im Rahmen ihres Arbeitsverhältnisses verpflichtet, die relevanten datenschutzrechtlichen Bestimmungen sowie diese Datenschutzweisung einzuhalten.

3. Gegenstand

Gegenstand dieser Datenschutzweisung ist die Bearbeitung von Personendaten, unabhängig von der Art und Form der Bearbeitung (d.h. auf Papier, digital, mündlich sowie vollständig-, teilweise- oder nicht-automatisiert).

4. Begriffe

Das anwendbare Datenschutzrecht definiert einige wichtige Begriffe. Grundsätzlich haben die nachfolgenden Begriffe die gleiche Bedeutung, wie sie im Bundesgesetz über den Datenschutz (**DSG**) definiert werden. Die wichtigsten Begriffe haben folgende Bedeutung:

Personendaten: Personendaten sind alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen.

Beispiele: *Name, Anschrift, Standortdaten, Online-Identifikatoren wie z.B. Geräte-ID, Cookie-ID, IP-Adresse, RFID-Tags etc.*

Merke: Es handelt sich um natürliche Personen und nicht um juristische Personen oder andere Einrichtungen. **Aber:** Informationen über eine Kontaktperson eines Lieferanten oder bei einer anderen B2B-Beziehung gelten ebenfalls als Personendaten.

Besonders schützenswerte Personendaten: Personendaten der folgenden Kategorien:

– Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten;

– Daten über die Gesundheit, die Intimsphäre oder die Zugehörigkeit zu einer Rasse oder Ethnie;

– genetische Daten;

– biometrische Daten, die eine natürliche Person eindeutig identifizieren;

– Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen; und

– Daten über Massnahmen der sozialen Hilfe.

Beispiele: *Aufnahmen von Videoüberwachungssystemen, Daten über die Gesundheit von Mitarbeitenden, Strafregisterauszüge von Mitarbeitenden etc.*

Betroffene Person: Jede natürliche Person, über die Personendaten bearbeitet werden.

Beispiele: *Kunden, Mitarbeitende, Partner bzw. Kontaktpersonen bei Partnern, Lieferanten bzw. Kontaktpersonen bei Lieferanten etc.*

Bearbeiten: Die Bearbeitung von Personendaten umfasst jeden Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren.

Beispiele: *das Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten von Daten.*

5. Grundsätze für die Bearbeitung von Personendaten

Das Unternehmen sowie alle Mitarbeitenden beachten bei der Bearbeitung von Personendaten folgende Grundsätze:

5.1 Rechtmässigkeit, Bearbeitung nach Treu und Glauben, Transparenz

Personendaten müssen auf rechtmässige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise bearbeitet werden. Die "Nachvollziehbarkeit" verlangt insbesondere, dass die Beschaffung von Personendaten sowie der Umfang und Zweck der Bearbeitung für die betroffene Person transparent ist (z.B. mittels einer Datenschutzerklärung mit den notwendigen Informationen über die jeweilige Bearbeitung). Bei jedem Umgang mit Personendaten haben Mitarbeitende folglich zu prüfen, ob die betroffenen Personen hierüber und über die weiteren Angaben nach Ziff. 8./9. informiert wurden.

Praktische Anweisung:

Vor der Bearbeitung von Personendaten haben sich die Mitarbeitenden zu vergewissern, ob die Bearbeitung rechtmässig ist, d.h., ob die Grundsätze der Bearbeitung von Personendaten, wie sie in dieser und in Ziffer 8.9. festgehalten sind, eingehalten werden und ob gegebenenfalls eine Einwilligung von der betroffenen Person eingeholt werden muss. Zudem müssen die Mitarbeitenden sicherstellen, dass die betroffenen Personen vor der Bearbeitung der Daten transparent über die entsprechende Bearbeitung der Personendaten informiert wurden.

Bestehen Zweifel, ob diese Voraussetzungen erfüllt sind, hat die Bearbeitung zu unterbleiben, bis die Datenschutzkoordinationsstelle die Rechtmässigkeit bestätigt hat. Ausgenommen sind Bearbeitungen, die in anderen Weisungen explizit für rechtmässig erklärt wurden.

5.2 Zweckbindung

Personendaten dürfen nur für festgelegte, eindeutige und, sofern auf die Datenbearbeitung die DSGVO anwendbar ist, rechtmässige Zwecke erhoben werden und eine Weiterbearbeitung darf nur im Rahmen dieses Zwecks erfolgen. Die Bearbeitung von Daten, für welche – beispielsweise in einer Datenschutzerklärung – kein Zweck festgelegt wurde, ist somit nicht zulässig. Sollen Daten zu einem anderen als dem festgelegten Zweck weiterbearbeitet werden, haben die Mitarbeitenden zu prüfen, ob der neue Zweck noch vom ursprünglichen Zweck miterfasst wird, d.h. mit dem ursprünglichen Zweck kompatibel ist.

Unter gewissen Umständen können Personendaten zu weiteren Zwecken, die über den ursprünglichen Bearbeitungszweck zum Zeitpunkt der Datenerhebung hinausgehen, bearbeitet werden. Um festzustellen, ob die Bearbeitung mit einem anderen Zweck als dem ursprünglichen vereinbar ist, berücksichtigt das Unternehmen unter anderem:

– jede Verbindung zwischen den Zwecken, für die die Personendaten erhoben wurden, und den Zwecken der beabsichtigten Weiterbearbeitung;

– den Zusammenhang, in dem die Personendaten erhoben wurden, insbesondere hinsichtlich des Verhältnisses zwischen den betroffenen Personen und der Verantwortlichen;

– die Art der Personendaten, insbesondere ob besonders schützenswerte Personendaten bearbeitet werden;

– die möglichen Folgen der beabsichtigten Weiterbearbeitung für die betroffenen Personen; und

– das Vorhandensein geeigneter Garantien und weiterer Massnahmen wie zum Beispiel Verschlüsselung oder Pseudonymisierung.

Praktische Anweisung:

Für die Beurteilung der Rechtmässigkeit einer weitergehenden Bearbeitung von Personendaten ist vor Beginn der Bearbeitung die Datenschutzkoordinationsstelle hinzuzuziehen und deren Zustimmung für die Bearbeitung einzuholen.

Die Datenschutzkoordinationsstelle vermerkt die Grundlage für die Bearbeitung der betreffenden Personendaten.

5.3 Datenminimierung

Die Bearbeitung von Personendaten muss für den festgelegten Zweck angemessen, erheblich und auf diesen beschränkt sein. Es dürfen deshalb nicht mehr Daten erhoben bzw. bearbeitet werden als es für den Bearbeitungszweck notwendig ist.

Praktische Anweisung:

Vor der Bearbeitung von Personendaten muss geprüft werden, ob diejenigen Daten, die im Zusammenhang mit der Bearbeitung erhoben bzw. bearbeitet werden sollen, auch zwingend für die Bearbeitung notwendig sind. Ist dies nicht der Fall, dürfen diese Personendaten nur unter der Voraussetzung einer gültigen Einwilligung der betroffenen Personen bearbeitet werden.

Beispiele:

1. *Auf der Hotelwebseite besteht die Möglichkeit sich an den Newsletter anzumelden. Dabei werden die Anrede, der Name und die E-Mailadresse erhoben und als zwingende Angaben gekennzeichnet. Für den Versand eines Newsletters wäre es jedoch ausreichend, wenn der Gast die E-Mailadresse angibt. Um dem Grundsatz der Datenminimierung zu entsprechen, darf somit nur die E-Mailadresse als zwingende Angabe erhoben werden. Die Anrede und der Name dürften nur auf freiwilliger Basis erhoben werden.*

2. *Im Hotel muss der Gast einen Meldeschein ausfüllen. Dabei werden neben der Anrede, dem Namen, der Adresse und den weiteren gesetzlich vorgeschriebenen Angaben auch die Interessen des Gastes als zwingende Angaben gekennzeichnet. Für die Erfüllung der Meldepflicht wäre es jedoch ausreichend, wenn der Gast einzig die gesetzlich zwingend zu erhebenden Daten angibt. Um dem Grundsatz der Datenminimierung zu entsprechen, dürfen somit nur die gesetzlich vorgeschriebenen Angaben erhoben werden. Die anderen Informationen des Gastes dürften nur auf freiwilliger Basis erhoben werden.*

Bestehen Zweifel, ob gewisse Daten als zwingende Angaben erhoben werden dürfen, hat die Bearbeitung zu unterbleiben, bis die Datenschutzkoordinationsstelle den Einzelfall analysiert und darüber entschieden hat. Ausgenommen sind Bearbeitungen, die in anderen Weisungen explizit für rechtmässig erklärt wurden.

5.4 Richtigkeit der Personendaten

Personendaten müssen sachlich richtig und auf dem neuesten Stand sein. Eine aktive Nachforschungspflicht bezüglich der Richtigkeit der Daten besteht allerdings nicht. Bestehen jedoch begründete Anhaltspunkte, dass Personendaten nicht mehr aktuell sein könnten, muss diesem Verdacht nachgegangen werden und die betroffenen Daten müssen gegebenenfalls berichtigt werden.

Praktische Anweisung:

Mitarbeitende, die auf unrichtige Daten aufmerksam werden, teilen dies dem Vorgesetzten mit oder berichtigen diese selbständig, sofern sie über die entsprechenden Bearbeitungsrechte verfügen und keine Zweifel an der Unrichtigkeit bestehen.

5.5 Speicherbegrenzung

Personendaten müssen in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie bearbeitet werden, erforderlich ist. Daten, die nicht mehr benötigt werden, sind deshalb zu löschen oder zu anonymisieren.

Die Frage, nach Ablauf welcher Dauer Daten nicht mehr benötigt werden, lässt sich nicht verallgemeinern und ist in bereichsspezifischen Weisungen festzulegen oder im Einzelfall zu beurteilen. Das Unternehmen sowie alle Mitarbeitenden des Unternehmens speichern Personendaten nicht länger als es für die Zwecke, zu denen sie ursprünglich erhoben oder später weiterbearbeitet wurden, notwendig ist.

Praktische Anweisung:

Was als notwendige Dauer der Speicherung gilt, hängt von den Umständen im Einzelfall ab und wird mit Unterstützung der Datenschutzkoordinationsstelle bestimmt.

5.6 Integrität und Vertraulichkeit (Datensicherheit)

Personendaten müssen in einer Weise bearbeitet werden, die eine angemessene Sicherheit der Personendaten gewährleistet. Sie müssen daher durch geeignete technische und organisatorische Massnahmen vor unbefugter oder unrechtmässiger Bearbeitung und vor unbeabsichtigtem Verlust und unbeabsichtigter Zerstörung oder Schädigung geschützt werden. Die Mitarbeitenden haben insbesondere sicherzustellen, dass andere Personen, wozu auch Mitarbeitende zu zählen sind, nicht auf Personendaten zugreifen oder diese bearbeiten können, solange deren Berechtigung nicht eindeutig feststeht.

Praktische Anweisung:

Jeder Mitarbeitende trägt dazu bei, dass im Unternehmen die Datensicherheit eingehalten wird. Wird festgestellt, dass die Integrität oder Vertraulichkeit der Personendaten verletzt wurde (z.B. durch die Versendung einer E-Mail mit einer Kundenliste an einen falschen Empfänger, bei Verdacht auf eine Phishing-Mail etc.), muss die Datenschutzkoordinationsstelle umgehend benachrichtigt werden. Die Datenschutzkoordinationsstelle entscheidet über das weitere Vorgehen.

5.7 Dokumentationspflicht

Die Unternehmensleitung bzw. die Hoteldirektion sorgt dafür, dass die genannten Grundsätze für alle Personendaten eingehalten werden. Sie ist verpflichtet deren Einhaltung jederzeit in dokumentierter Art und Weise nachweisen zu können.

5.8 Einwilligungen

Das Unternehmen holt die notwendigen Einwilligungen der betroffenen Personen rechtzeitig, d.h. bevor eine Bearbeitung vorgenommen wird, für die eine Einwilligung notwendig ist, ein.

Sofern die Einwilligung ausdrücklich erfolgen muss, hat die Einwilligung durch eine eindeutige bestätigende Handlung, mit der freiwillig, für den konkreten Fall, in informierter Weise und unmissverständlich zu erfolgen, mit der die betroffene Person ausdrücklich zum Ausdruck bringt, mit der Bearbeitung der sie betreffenden Personendaten einverstanden zu sein.

Eine Einwilligungserklärung wird in verständlicher und leicht zugänglicher Form und in einer klaren, einfachen Sprache zur Verfügung gestellt. Sie ist von anderen Angelegenheiten klar unterscheidbar und beinhaltet keine missbräuchlichen Klauseln.

Zudem wird der betroffenen Person eine einfache Methode zur Verfügung gestellt, mit der sie ihre Einwilligung jederzeit widerrufen kann.

Praktische Anweisung:

Bei der Beurteilung, ob die Anforderungen an die Einwilligung erfüllt sind, sind insbesondere die weiteren Weisungen zu beachten.

Bestehen Zweifel, so nehmen die Mitarbeitenden die Datenbearbeitung so lange nicht vor, bis die Datenschutzkoordinationsstelle die Einhaltung der Vorgaben bestätigt hat.

6. Besondere Bearbeitungstätigkeiten

6.1 Bearbeitung von besonders schützenswerten Personendaten

Das Unternehmen sowie alle Mitarbeitenden bearbeiten besonders schützenswerte Personendaten ausschliesslich nach Rücksprache mit der Datenschutzkoordinationsstelle, unter nachfolgenden Voraussetzungen und nur soweit der Bearbeitung keine gesetzlichen Regelungen entgegenstehen:

– die betroffene Person hat in die Bearbeitung der Daten für einen oder mehrere festgelegte Zwecke ausdrücklich eingewilligt;

– die Bearbeitung ist erforderlich, damit das Unternehmen oder die betroffene Person die ihr aus dem Arbeitsrecht und dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechte ausüben oder ihren diesbezüglichen Pflichten nachkommen kann;

– die Bearbeitung bezieht sich auf Personendaten, die die betroffene Person offensichtlich öffentlich gemacht hat; oder

– die Bearbeitung ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder bei Handlungen vor Gerichten erforderlich.

Die Mitarbeitenden bearbeiten besonders schützenswerte Personendaten so lange nicht, bis die Datenschutzkoordinationsstelle die Rechtmässigkeit der Bearbeitung bestätigt hat.

Praktische Anweisung:

Vor der Bearbeitung von besonders schützenswerten Personendaten wird jeweils die Datenschutzkoordinationsstelle beigezogen und deren Zustimmung zur Bearbeitung eingeholt sowie die Grundlage für die Bearbeitung der betreffenden Personendaten vermerkt.

Das Unternehmen wendet bei der Bearbeitung von besonders schützenswerten Personendaten erhöhte Sicherheitsmassnahmen an.

6.2 Bearbeitung von Personendaten eines Kindes

Personendaten eines Kindes werden grundsätzlich nur bearbeitet, wenn dass Kind das sechzehnte Lebensjahr vollendet hat. Hat das Kind das sechzehnte Lebensjahr noch nicht vollendet,

werden dessen Personendaten nur bearbeitet, sofern und soweit die Einwilligung zur Bearbeitung durch den gesetzlichen Vertreter des Kindes erteilt wurde.

Das Unternehmen sowie alle Mitarbeitenden unternehmen angemessene Anstrengungen, um sich in solchen Fällen zu vergewissern, dass die Einwilligung durch den gesetzlichen Vertreter des Kindes erteilt wurde.

Praktische Anweisung:

Bestehen Zweifel, ob die Anforderungen an die Einwilligung durch den gesetzlichen Vertreter erfüllt sind, nehmen die Mitarbeitenden die Datenbearbeitung so lange nicht vor, bis die Datenschutzkoordinationsstelle die Einhaltung der Vorgaben bestätigt hat.

6.3 Digitales Marketing

Es werden keine Mitteilungen zu Werbe- oder Marketingzwecken an Kontakte (Kunden, Lieferanten usw.) über digitale Medien wie E-Mail, Internet oder Mobiltelefone versandt, ohne vorher die Einwilligung der betroffenen Personen einzuholen. Wenn eine Einwilligung zur Bearbeitung von Personendaten zu digitalen Marketingzwecken vorliegt, wird die betroffene Person in jeder Mitteilung darüber informiert, dass sie das Recht hat, ihre Einwilligung jederzeit zu widerrufen.

Praktische Anweisung:

Bestehen Zweifel, ob eine Mitteilung Werbecharakter hat, eine Einwilligung vorliegt oder die Einwilligung widerrufen wurde, hat die Datenbearbeitung so lange zu unterbleiben, bis die Datenschutzkoordinationsstelle die Einhaltung der Vorgaben an das digitale Marketing bestätigt hat.

Good Practice:

Folgendes ist nicht erlaubt:

- vorangekreuzte Opt-in-Boxen;
- auf Schweigen, Inaktivität, Standardeinstellungen oder Ihre Allgemeinen Geschäftsbedingungen vertrauen; und
- nur eine Opt-out-Wahl ohne explizites Opt-in zu verlangen.

Folgendes muss sichergestellt werden:

- es werden Aufzeichnungen über das Einwilligungsverfahren geführt (z.B. Datum der Einwilligung, Art der Einwilligung, welche Informationen der betroffenen Person zur Verfügung gestellt wurden);
- die Einwilligung zur Bearbeitung ist unterscheidbar, klar und nicht mit anderen schriftlichen Vereinbarungen oder Erklärungen verbunden. Es wird eine gesonderte Einwilligung für verschiedene Bearbeitungsvorgänge eingeholt (die Einwilligung zur Direktvermarktung darf nie mit anderen Einwilligungen zur Bearbeitung verknüpft sein);

- betroffene Personen werden darüber informiert, dass sie das Recht haben, ihre Einwilligung jederzeit zu widerrufen; und

- systemtechnisch sind einfache Methoden vorgesehen, um die Einwilligung zu widerrufen.

Beachte: Für Bestandeskunden können gewisse Privilegierungen gelten, die im Einzelfall gemeinsam mit der Datenschutzkoordinationsstelle geprüft werden müssen.

7. Verzeichnis über die Bearbeitungstätigkeiten

Das Unternehmen und gegebenenfalls deren Vertreter führen ein Verzeichnis über alle Bearbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen. Dieses enthält mindestens folgende Angaben:

– Die Identität des Verantwortlichen, d.h. den Namen und die Kontaktdaten des Unternehmens und gegebenenfalls der gemeinsam mit ihm Verantwortlichen, gegebenenfalls ihres Vertreters sowie gegebenenfalls des Datenschutzbeauftragten;

– die Zwecke der Bearbeitung;

– eine Beschreibung der Kategorien betroffener Personen und der Kategorien der bearbeiteten Personendaten;

– die Kategorien von Empfängern, gegenüber denen die Personendaten offengelegt worden sind oder noch offengelegt werden (einschliesslich Empfänger in Drittländern oder internationale Organisationen);

– wenn möglich, die Aufbewahrungsdauer der Personendaten oder die Kriterien zur Festlegung dieser Dauer;

– wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Massnahmen; und

– falls die Daten ins Ausland bekanntgegeben werden, die Angabe des Staates und die implementierten Garantien zur Sicherstellung eines angemessenen Datenschutzniveaus.

Praktische Anweisung:

Damit das Verzeichnis über die Bearbeitungstätigkeiten stets aktuell bleibt, melden die Mitarbeitenden der Datenschutzkoordinationsstelle neue Bearbeitungstätigkeiten, die die oben aufgeführten Informationen enthalten müssen, bevor diese in das Verzeichnis aufgenommen werden.

8. Informationspflichten bei der Erhebung von Personendaten direkt bei der betroffenen Person

Zum Zeitpunkt der Erhebung der Personendaten müssen den betroffenen Personen insbesondere folgende Informationen vom Unternehmen mitgeteilt werden:

– die Identität und die Kontaktdaten des Unternehmens;

– die Bearbeitungszwecke; und

– gegebenenfalls die Empfänger oder Kategorien von Empfängern der Personendaten.

– Bei der Bekanntgabe von Personendaten ins Ausland: den Staat oder das internationale Organ und gegebenenfalls die Garantien zur Sicherstellung eines angemessenen Datenschutzniveaus oder die Anwendung einer Ausnahme zur Sicherstellung eines angemessenen Datenschutzniveaus.

– Bei der Vornahme von sog. automatisierten Einzelentscheidungen: die Möglichkeit der betroffenen Person ihren Standpunkt über die Entscheidung, die ohne menschlichen Einfluss gefällt wird, dazulegen, sowie die Möglichkeit zur Überprüfung der automatisierten Einzelentscheidung durch eine natürliche Person.

Gegebenenfalls kann das anwendbare Datenschutzrecht darüberhinausgehende Inhalte vorsehen, so z.B. das europäische Datenschutzrecht, das zusätzlich vorsieht, dass folgende Angaben in den Informationen enthalten sein müssen:

– die Rechtsgrundlage für die Bearbeitung;

– gegebenenfalls die Absicht, die Personendaten in ein Drittland zu übermitteln sowie das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der EU-Kommission, einen Verweis auf die geeigneten oder angemessenen Garantien und die Angaben, wie eine Kopie von ihnen zu erhalten ist oder wo sie verfügbar sind;

– die Dauer, für die die Personendaten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;

– das Bestehen des Rechts auf Auskunft über die betreffenden Personendaten sowie bezüglich die Rechte der Berichtigung, Löschung, Einschränkung der Bearbeitung oder Widerspruchs gegen die Bearbeitung sowie des Rechts auf Datenübertragbarkeit;

– gegebenenfalls das Bestehen des Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmässigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Bearbeitung berührt wird;

– das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde; und

– gegebenenfalls das Bestehen einer automatisierten Entscheidungsfindung einschliesslich Profiling und im letzteren Fall aussagekräftige Informationen über die involvierte Logik, die Tragweite und die angestrebten Auswirkungen einer derartigen Bearbeitung für die betroffene Person.

Diese Informationen werden den betroffenen Personen in der Regel mittels einer Datenschutzerklärung zur Verfügung gestellt.

Praktische Anweisung:

Damit die Informationen gegenüber den betroffenen Personen stets aktuell bleiben, melden die Mitarbeitenden der Datenschutzkoordinationsstelle neue Bearbeitungstätigkeiten, bevor diese aufgenommen werden, die die oben aufgeführten Informationen enthalten müssen.

9. Informationspflichten bei der indirekten Erhebung von Personendaten

Personendaten über betroffene Personen können auch indirekt, d.h. bei Dritten, erhoben werden. Diese entbindet das Unternehmen jedoch nicht davon, die betroffene Person über die Bearbeitung zu informieren. Zusätzlich zu den unter Ziffer 8 aufgelisteten Informationen, teilt das Unternehmen der betroffenen Person die Kategorien der bearbeiteten Personendaten mit. Die Information muss der betroffenen Person spätestens einen Monat nach dem das Unternehmen die Personendaten vom Dritten erhalten hat, mitgeteilt werden oder spätestens im Zeitpunkt der Bekanntgabe an einen Dritten, falls die Bekanntgabe vor der einmonatigen Frist erfolgt.

Gegebenenfalls kann das anwendbare Datenschutzrecht darüberhinausgehende Inhalte vorsehen), so z.B. das europäische Datenschutzrecht, das zusätzlich zu Ziffer 8 oben vorsieht, dass folgende Angaben in den Informationen enthalten sein müssen:

– aus welcher Quelle die Personendaten stammen; und

– gegebenenfalls, ob sie aus öffentlich zugänglichen Quellen stammen.

Praktische Anweisung:

Damit die Informationen gegenüber den betroffenen Personen stets aktuell bleiben, melden die Mitarbeitenden der Datenschutzkoordinationsstelle neue Bearbeitungstätigkeiten, bevor diese aufgenommen werden, die die oben aufgeführten Informationen enthalten müssen.

10. Rechte der betroffenen Personen

Das Unternehmen sowie alle Mitarbeitenden beachten folgende Rechte der betroffenen Personen:

10.1 Auskunftsrecht

Jede betroffene Person hat das Recht vom Unternehmen eine Bestätigung darüber zu verlangen, ob Personendaten über sie bearbeitet werden. Eingehende Auskunftsbegehren werden umgehend an die Datenschutzkoordinationsstelle weitergeleitet, sofern diese nicht bei dieser eingegangen sind.

Vor der Beantwortung der Anfrage muss zwingend die Identität der betroffenen Person überprüft werden. Kann die Identität zweifelsfrei festgestellt werden, hat die betroffene Person das Recht, die folgenden Informationen bezüglich ihrer eigenen Personendaten zu erhalten:

– die Identität und die Kontaktdaten des Verantwortlichen;

– die bearbeiteten Personendaten als solche;

– die Bearbeitungszwecke;

– die Aufbewahrungsdauer der Personendaten oder, falls dies nicht möglich ist, die Kriterien zur Festlegung dieser Aufbewahrungsdauer;

– die verfügbaren Angaben über die Herkunft der Personendaten, soweit sie nicht bei der betroffenen Person selbst beschafft wurden;

– gegebenenfalls das Vorliegen einer automatisierten Einzelentscheidung sowie die Logik, auf der die Entscheidung beruht;

– gegebenenfalls die Empfänger oder die Kategorien von Empfängern, denen Personendaten bekanntgegeben werden, sowie den Staat oder das internationale Organ und gegebenenfalls die Garantien zur Sicherstellung eines angemessenen Datenschutzniveaus oder die Anwendung einer Ausnahme zur Sicherstellung eines angemessenen Datenschutzniveaus.

Gegebenenfalls kann das anwendbare Datenschutzrecht darüberhinausgehende Inhalte vorsehen, so z.B. das europäische Datenschutzrecht, das zusätzlich vorsieht, dass der betroffenen Person folgende Informationen mitgeteilt werden müssen:

– das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden Personendaten oder auf Einschränkung der Bearbeitung durch den Verantwortlichen oder eines Widerspruchsrechts gegen diese Bearbeitung;

– das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;

– das Bestehen einer automatisierten Entscheidungsfindung einschliesslich Profiling und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik und die angestrebten Auswirkungen einer derartigen Bearbeitung für die betroffene Person.

Das Unternehmen stellt eine Kopie der Personendaten, die Gegenstand der Bearbeitung sind, in einem gängigen strukturierten und maschinenlesbaren Format zur Verfügung.

Durch die Weitergabe der angefragten Informationen an die betroffene Person könnten unter Umständen Personendaten einer anderen betroffenen Person offengelegt werden. In solchen Fällen müssen die andere Personen betreffende Informationen redigiert oder zurückbehalten werden, je nachdem was notwendig oder angemessen erscheint, um die Rechte dieser Person zu schützen.

Praktische Anweisung: Anfragen von betroffenen Personen auf Auskunft über ihre Personendaten sind umgehend an die Datenschutzkoordinationsstelle weiterzuleiten.

10.2 Recht auf Berichtigung

Die betroffene Person hat das Recht, vom Unternehmen unverzüglich die Berichtigung sie betreffender unrichtiger Personendaten zu verlangen. Unter Berücksichtigung der Zwecke der Bearbeitung hat die betroffene Person das Recht, die Vervollständigung unvollständiger Personendaten – auch mittels einer ergänzenden Erklärung – zu verlangen.

Praktische Anweisung:

Anfragen von betroffenen Personen auf Berichtigung ihrer Personendaten sind umgehend an die Datenschutzkoordinationsstelle weiterzuleiten.

Anfragen von betroffenen Personen auf Berichtigung von Mitarbeiterdaten sind an die Personalabteilung des Unternehmens zu richten.

10.3 Recht auf Löschung (Recht auf Vergessen werden)

Die betroffene Person hat unter bestimmten Voraussetzungen das Recht, vom Unternehmen zu verlangen, dass sie betreffende Personendaten unverzüglich gelöscht werden. Das Unternehmen ist verpflichtet, allfällige Auftragsbearbeiter über die Löschung zu informieren und diese gegebenenfalls zur Löschung zu verpflichten. Handelt das Unternehmen selbst als Auftragsbearbeiterin, hat sie unverzüglich die Verantwortliche über das Gesuch um Löschung zu informieren.

Praktische Anweisung:

Anfragen von betroffenen Personen auf Löschung ihrer Personendaten sind umgehend der Datenschutzkoordinationsstelle weiterzuleiten.

Anfragen von betroffenen Personen auf Löschung von Mitarbeiterdaten sind an die Personalabteilung des Unternehmens zu richten.

10.4 Recht auf Einschränkung der Bearbeitung

Eine betroffene Person hat das Recht, die Einschränkung der Bearbeitung ihrer Personendaten zu verlangen, wenn eine der folgenden Voraussetzungen gegeben ist:

– die Richtigkeit der Personendaten wird von der betroffenen Person bestritten (inkl.). Die Einschränkung der Bearbeitung erfolgt unter Eintragung eines Bestreitungsvermerks für eine Dauer, die es dem Unternehmen ermöglicht, die Richtigkeit der Personendaten zu überprüfen;

– die Bearbeitung ist unrechtmässig und die betroffene Person verlangt statt der Löschung eine Einschränkung der Nutzung ihrer Personendaten;

– das Unternehmen benötigt die Personendaten für die Zwecke der Bearbeitung nicht länger. Die betroffene Person benötigt sie jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen und verlangt statt der Löschung eine Einschränkung der Nutzung ihrer Personendaten; oder

– die betroffene Person hat Widerspruch gegen die Bearbeitung gemäss dem Widerspruchsrecht eingelegt. Die Einschränkung erfolgt so lange noch nicht feststeht, ob die berechtigten Gründe des Unternehmens oder die der betroffenen Person überwiegen.

Wurde die Bearbeitung eingeschränkt, so dürfen diese Personendaten – von ihrer Speicherung abgesehen – nur mit Einwilligung der betroffenen Person, zur Geltendmachung, Ausübung oder

Verteidigung von Rechtsansprüchen, zum Schutz der Rechte einer anderen natürlichen oder juristischen Person oder aus Gründen eines wichtigen öffentlichen Interesses bearbeitet werden.

Eine betroffene Person, die eine Einschränkung der Bearbeitung erwirkt hat, wird vom Unternehmen unterrichtet, bevor die Einschränkung aufgehoben wird.

Praktische Anweisung:

Anfragen von betroffenen Personen auf Einschränkung der Bearbeitung ihrer Personendaten sind umgehend an die Datenschutzkoordinationsstelle weiterzuleiten.

10.5 Datenübertragbarkeit (Datenportabilität)

Eine betroffene Person hat das Recht, die sie betreffenden Personendaten, die sie dem Unternehmen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten. Sie hat ferner das Recht zu verlangen, dass das Unternehmen diese Daten einer anderen Gesellschaft ohne Behinderung übermittelt, sofern:

– die Bearbeitung auf einer Einwilligung der betroffenen Person beruht;

– die Bearbeitung in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags zwischen dem Unternehmen und der betroffenen Person bearbeitet werden; oder

– die Bearbeitung mithilfe automatisierter Verfahren erfolgt.

Praktische Anweisung:

Anfragen von betroffenen Personen auf Übertragung ihrer Personendaten sind umgehend an die Datenschutzkoordinationsstelle weiterzuleiten.

10.6 Widerspruchsrecht

Eine betroffene Person hat das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Bearbeitung sie betreffender Personendaten Widerspruch einzulegen.

In solchen Fällen bearbeitet das Unternehmen die Personendaten nicht mehr, es sei denn, es kann zwingende schutzwürdige Gründe für die Bearbeitung nachweisen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen oder die der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen dienen.

Praktische Anweisung:

Bei der Geltendmachung des Widerspruchrechts durch die betroffene Person ist umgehend die Datenschutzkoordinationsstelle zu informieren.

10.7 Rechte bei automatisierten Einzelentscheidungen

Eine betroffene Person hat das Recht, dass eine Entscheidung, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt, nicht ausschliesslich auf einer automatisierten Bearbeitung beruht. Ausnahmen sind zulässig, soweit dies das Gesetz vorsieht.

Das Unternehmen wendet automatisierte Einzelentscheidungen, die den betroffenen Personen gegenüber rechtliche Wirkung entfalten nur an, wenn die Entscheidung für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Unternehmen erforderlich, aufgrund von anwendbaren gesetzlichen Vorschriften notwendig ist oder mit der ausdrücklichen Einwilligung der betroffenen Person erfolgt.

Als Entscheidungen in diesem Sinn gelten solche, die auf einer rein automatisierten Datenbearbeitung basieren und entweder rechtliche Wirkung gegenüber der betroffenen Person entfalten oder die die betroffene Person in ähnlicher Weise erheblich beeinträchtigen. Somit sind beispielsweise bei einer automatisierten Bonitätsprüfung, gestützt auf welcher ein Vertragsschluss mit einer Person gegebenenfalls abgelehnt wird, die Vorgaben dieser Ziffer zu beachten.

Als Profiling gilt jede Art der automatisierten Bearbeitung von Personendaten, die darin besteht, dass diese Personendaten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, zu analysieren oder vorherzusagen, insbesondere bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser betroffenen Person. Soweit das Profiling mit einer automatisierten Einzelentscheidung verbunden wird, die entweder rechtliche Wirkung gegenüber der betroffenen Person entfaltet oder die die betroffene Person in ähnlicher Weise erheblich beeinträchtigt, sind die Vorgaben dieser Ziffer ebenfalls zu beachten.

Das Unternehmen sorgt dafür, dass Profiling und automatisierte Einzelentscheidungen im Einzelfall auf korrekten Daten beruht.

Praktische Anweisung:

Die Mitarbeitenden verzichten so lange auf automatisierte Einzelentscheidungen, bis die Datenschutzkoordinationsstelle den Einsatz sowie die Modalitäten derselben für rechtmässig erklärt hat.

10.8 Vorgehen bei Gesuchen von betroffenen Personen

Praktische Anweisung:

Für den Fall, dass Auskunfts-, Löschungs- und Berichtigungsgesuche sowie Anträge auf Datenübertragbarkeit, Widerruf von Einwilligungen und Widersprüche gegen die Datenbearbeitung aufgrund berechtigter Interessen nicht automatisch bei der Datenschutzkoordinationsstelle eingehen, werden diese unverzüglich an die Datenschutzkoordinationsstelle weitergeleitet.

Den Mitarbeitenden ist es untersagt, Anfragen von betroffenen Personen zu bearbeiten und mit betroffenen Personen ohne vorgängige Abstimmung mit der Datenschutzkoordinationsstelle zu kommunizieren.

11. Übermittlung Personendaten an Dritte

11.1 Grundsatz

Eine Übermittlung von Personendaten ins Ausland ist grundsätzlich zulässig, wenn für das betreffende Drittland oder für die betreffende internationale Organisation ein angemessenes Datenschutzniveau sichergestellt werden kann. Ein angemessenes Datenschutzniveau eines Staates liegt dann vor, wenn dies durch die zuständige Behörde festgestellt wurde (in der Schweiz durch den Bundesrat und in der EU durch die EU-Kommission).

Falls Personendaten in Drittländer ohne angemessenes Datenschutzniveau übermittelt werden sollen, sind entsprechende geeignete Garantien einzusetzen. Eine diesbezügliche Übermittlung ist nur nach vorgängiger Prüfung und mit Zustimmung der Datenschutzkoordinationsstelle zulässig.

11.2 Übermittlungen zwischen Gruppengesellschaften

Gruppengesellschaften des Unternehmens stellen datenschutzrechtlich untereinander sogenannte Dritte dar. Als Grundlage für ein gruppenweit einheitliches Vorgehen schliessen die Gesellschaften einen Intercompany-Vertrag ab, wobei die Gruppengesellschaften sowohl Verantwortliche (Controller) als auch Auftragsbearbeiter (Processor) sein können. Der Intercompany-Vertrag regelt die Verpflichtungen der Vertragsparteien entsprechend ihrer Rolle als Verantwortliche wie auch in ihrer Rolle als Auftragsbearbeiter.

11.3 Übermittlungen an sonstige Dritte

Das Unternehmen übermittelt Personendaten ausschliesslich dann an Dritte und gewährt Dritten Zugang zu Personendaten, wenn garantiert ist, dass die Daten vom Empfänger rechtmässig bearbeitet und angemessen geschützt werden:

– Wenn der **Dritte als Verantwortlicher** gilt, schliesst das Unternehmen einen Vertrag mit dem Verantwortlichen ab, in dem die Verantwortlichkeiten bezüglich der übermittelten Personendaten jeder Partei definiert werden.

– Wenn der **Dritte als Auftragsbearbeiter** gilt, schliesst das Unternehmen einen entsprechenden Auftragsdatenbearbeitungsvertrag mit dem Auftragsbearbeiter ab. Der Auftragsdatenbearbeitungsvertrag verpflichtet den Auftragsbearbeiter, die datenschutzrechtlichen Grundsätze einzuhalten, insbesondere wird er verpflichtet, die Daten vor einer weiteren Offenlegung zu schützen, diese nur gemäss den Weisungen des Unternehmens zu bearbeiten, angemessene technische und organisatorische Massnahmen zum Schutz der Personendaten zu implementieren und Verletzungen der Datensicherheit zu melden.

12. Technische und organisatorische Massnahmen

Das Unternehmen trifft angemessene technische und organisatorische Massnahmen, um die Sicherheit der Personendaten gemäss den anwendbaren datenschutzrechtlichen Vorschriften zu gewährleisten. Verletzungen der Datensicherheit wie z.B. ein Hackerangriff sind umgehend der Datenschutzkoordinationsstelle zu melden. Der Umgang mit solchen Verletzungen richtet sich nach einer gesonderten die Informationssicherheit betreffende Weisung.

13. Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

Das Unternehmen stellt sicher, dass die datenschutzrechtlichen Grundsätze bereits frühzeitig in neuen Projekten berücksichtigt werden und jeweils in die technische Umsetzung einfliessen (Privacy by Design).

Das Unternehmen trifft zudem geeignete technische und organisatorische Massnahmen, damit durch Voreinstellungen sichergestellt werden kann, dass nur Personendaten, deren Bearbeitung für den jeweiligen Bearbeitungszweck erforderlich sind, bearbeitet werden. Dazu wird insbesondere sichergestellt, dass die jeweiligen Voreinstellungen datenschutzfreundlich ausgestaltet sind (Privacy by Default).

Praktische Anweisung:

Bei der Planung und Implementierung neuer Prozesse und Systemapplikationen, wird die Datenschutzkoordinationsstelle möglichst frühzeitig miteinbezogen, sodass die Grundsätze des Privacy by Design und Privacy by Default angemessen im Projekt berücksichtigt werden können.

14. Datenschutz-Folgenabschätzung

Das Unternehmen führt vorab eine Abschätzung der Folgen von vorgesehenen Bearbeitungsvorgängen durch (Datenschutz-Folgenabschätzung), wenn eine geplante Bearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen mit sich bringen kann.

Die Prüfung, ob eine Datenschutz-Folgenabschätzung erforderlich ist, hat insbesondere bei der Verwendung neuer Technologien oder bei neuartigen Datenbearbeitungsvorgängen, sowie aus der Art, dem Umfang, den Umständen und dem Zweck der Bearbeitung zu erfolgen wie z.B. bei umfangreichen Bearbeitungen von besonders schützenswerten Daten oder bei der systematischen und umfangreichen Videoüberwachung von öffentlich zugänglichen Bereichen.

Praktische Anweisung:

Das Unternehmen holt für die Prüfung, ob die Durchführung einer Datenschutz-Folgenabschätzung notwendig ist, den Rat der Datenschutzkoordinationsstelle ein. Die Durchführung von Datenschutz-Folgenabschätzungen erfolgt nach einer gesonderten internen Richtlinie.

15. Meldung von Verletzungen der Datensicherheit

Eine Verletzung der Datensicherheit liegt dann vor, wenn eine Verletzung der Sicherheit dazu führt, dass Personendaten unbeabsichtigt oder widerrechtlich verlorengehen, gelöscht, vernichtet, oder verändert werden oder Unbefugten offengelegt oder zugänglich gemacht werden.

Im Falle einer Verletzung der Datensicherheit meldet das Unternehmen möglichst unverzüglich, jedoch spätestens binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der zuständigen Aufsichtsbehörde, sofern die Verletzung des Schutzes der Personendaten voraussichtlich zu einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen führt. Das Unternehmen informiert die betroffenen Personen, wenn es zu ihrem Schutz erforderlich ist oder die zuständige Aufsichtsbehörde dies verlangt.

Praktische Anweisungen:

Wenn Mitarbeitende eine Verletzung der Datensicherheit erkennen oder vermuten, können sie dies über j.stiller@lenkerhof.ch melden.

Der Prozess zur internen Meldung einer Verletzung der Datensicherheit richtet sich nach einer gesonderten Richtlinie.

16. Verantwortlichkeiten

16.1 Geschäftsleitung bzw. Hoteldirektion

Die Geschäftsleitung bzw. die Hoteldirektion definiert die übergeordneten Grundsätze für die Gewährleistung des Datenschutzes im Unternehmen. Sie ernennt eine Person oder Abteilung – die Datenschutzkoordinationsstelle –, die mit der Durchsetzung der datenschutzrechtlichen Vorgaben beauftragt wird.

16.2 Vorgesetzte

Die Vorgesetzten aller Stufen sind in ihren Verantwortungsbereichen für die Durchsetzung und Einhaltung der datenschutzrechtlichen Bestimmungen verantwortlich. Sie sorgen in Zusammenarbeit mit der Datenschutzkoordinationsstelle für Schulung und Sensibilisierung ihrer Mitarbeitenden. Sie nehmen eine Vorbildfunktion wahr und fördern die Motivation der Mitarbeitenden, Massnahmen zum Datenschutz einzuhalten.

16.3 Datenschutzkoordinationsstelle

Die Geschäftsleitung hat eine Datenschutzkoordinationsstelle benannt. Die Datenschutzkoordinationsstelle ist die zentrale Anlaufstelle für Fragen des Datenschutzes und kann via j.stiller@lenkerhof.ch oder Telefon unter 033 736 36 36 kontaktiert werden.

Die Datenschutzkoordinationsstelle hat insbesondere folgende Aufgaben:

– sie trägt die Dokumentenverantwortung für diese Datenschutzweisung;

– sie unterstützt das Unternehmen bei der Durchsetzung und Umsetzung des Datenschutzes; und

– sie beobachtet und berücksichtigt die Entwicklung der gesetzlichen Vorgaben im Bereich des Datenschutzes.

Die Durchsetzung dieser Weisung obliegt ausschliesslich den Vorgesetzten und nicht der Datenschutzkoordinationsstelle.

Eine detaillierte Aufgabenbeschreibung ist im Pflichtenheft der Datenschutzkoordinationsstelle definiert.

17. Sanktionen

Verletzungen dieser Datenschutzweisung können disziplinarische Massnahmen und/oder zivil- und/oder strafrechtliche Massnahmen nach sich ziehen.

18. Schlussbestimmungen

18.1 Änderungen und Ergänzungen

Diese Datenschutzweisung kann nur schriftlich durch einen Beschluss der Geschäftsleitung bzw. der Hoteldirektion des Unternehmens abgeändert, ergänzt oder aufgehoben werden. Als Änderung oder Ergänzung ist jegliche Hinzufügung, Streichung oder Modifikation einzelner Bestimmungen zu qualifizieren. Ausgenommen hiervon sind Berichtigungen formeller Art.

18.2 Ergänzende Dokumente

Diese Datenschutzweisung stellt die Grundlage für die datenschutzrechtlichen Vorgaben des Unternehmens dar. Ergänzend zu dieser können weitere Dokumente, Weisungen und Prozesse erarbeitet werden, die im Zusammenhang mit der Bearbeitung von Personendaten notwendig sind.

18.3 Zugang zu dieser Weisung und Änderungen

Diese Datenschutzweisung ist allen Mitarbeitenden zugänglich und kann über Beekeeper digital heruntergeladen und angeschaut werden sowie beim HR in ausgedruckter Version bezogen werden.

18.4 Inkrafttreten

Diese Datenschutzweisung tritt am 1. September 2023 in Kraft.