Einleitende Bemerkung:

Die untenstehende Muster-Datenschutzrichtlinie fokussiert sich auf das Wesentliche und gibt eine mögliche Struktur vor. Es macht Sinn, diese gemäss Ihrer konkreten Unternehmenssituation zu ergänzen bzw. anzupassen. Dazu kann der Beizug eines Spezialisten sinnvoll sein.

* * * * *

Datenschutzrichtlinie

I. Allgemeines

1. Einleitung

1.1. Die im Unternehmen vorhandenen Datensind für das Unternehmen von grossem Wert. Diese Daten sind daher gegen unbefugte Zugriffe und andere Gefährdungen zu schützen.

1.2 Die Kunden, Partner und Mitarbeiter des Unternehmens erwarten, dass die dem Unternehmen anvertrauten Daten besonders geschützt werden und ein sorgsamer Umgang mit ihnen erfolgt.

1.3 [Bei Fragen zum Thema Datenschutz oder zum Umgang mit Personendaten kann der Datenschutzbeauftragte [Name, Emailadresse/Telefonnummer o.ä.] kontaktiert werden.]

1.4 […]

2. Ziel der Datenschutzrichtlinie

2.1 Mit dieser Datenschutzrichtlinie sollen einheitliche Standards für den Datenschutz im Unternehmen geschaffen werden.

2.2 Durch die Einhaltung der in dieser Datenschutzrichtlinie definierten Standards kommt das Unternehmen seinen datenschutzrechtlichen Verpflichtungen nach und sorgt für eine ausreichende Berücksichtigung der Interessen sowie Rechte der betroffenen Personen.

2.3 Die Beachtung dieser Datenschutzrichtlinie ist Voraussetzung für den sicheren Austausch von Personendaten innerhalb des Unternehmens und mit Dritten.

2.4 […]

3. Anwendungsbereich der Datenschutzrichtlinie

3.1 Diese Datenschutzrichtlinie gilt für jegliche Bearbeitung von Personendaten, wobei insbesondere das Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten von Daten erfasst werden. Sie findet Anwendung auf sämtliche Arten von Personendaten, insbesondere Daten von Mitarbeitern, Kunden, Lieferanten und anderen Geschäftspartnern.

3.2 Die Datenschutzrichtlinie beschreibt, konkretisiert bzw. ergänzt dabei auch gesetzliche Vorgaben, namentlich solche aus dem Schweizer Datenschutzgesetz (DSG).

3.3 […]

4. Definitionen

4.1 **Personendaten** im Sinne dieser Unternehmensrichtlinie sind alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen.

4.2 **Betroffene Personen** sind diejenigen natürlichen Personen, über die Personendaten bearbeitet werden.

4.3 **Verantwortlicher** ist eine private Person, die allein oder zusammen mit anderen über den Zweck und die Mittel der Bearbeitung entscheidet.

4.4 **Auftragsbearbeiter** ist ein Dritter, der im Auftrag des Verantwortlichen Personendaten bearbeitet.

[…]

II. Grundregeln der Datenbearbeitung

5. Rechtmässigkeit

5.1 Personendaten müssen rechtmässig bearbeitet werden. Die Bearbeitung gilt nur als rechtmässig, wenn sie durch (a) Einwilligung der betroffenen Person, durch (b) ein überwiegendes privates oder öffentliches Interesse oder durch (c) Gesetz gerechtfertigt ist.

6. Transparenz

6.1 Die Bearbeitung der Daten muss grundsätzlich so erfolgen, dass sie der betroffenen Person bekannt ist.

7. Verhältnismässigkeit

7.1 Bei der Bearbeitung von Personendaten ist der Grundsatz der Verhältnismässigkeit zu beachten. Gemäss diesem Grundsatz dürfen nur solche Daten erhoben werden, die für den entsprechenden Zweck *notwendig* und *geeignet* sind.

7.2 Weiter dürfen Personendaten nur so lange gespeichert werden, wie dies für den Zweck notwendig ist (vgl. hiernach).

8. Zweckbindung

8.1 Personendaten dürfen nur zu einem bestimmten und für die betroffene Person erkennbaren Zweck beschafft werden; sie dürfen nur so bearbeitet werden, dass es mit diesem Zweck vereinbar ist.

8.2 Werden die Personendaten zum Zweck der Bearbeitung nicht mehr benötigt, müssen diese vernichtet oder anonymisiert werden.

9. Richtigkeit

9.1 Alle Mitarbeiter haben darauf zu achten, dass Personendaten richtig sind und auf dem neuesten Stand gehalten werden.

9.2 Es müssen alle angemessenen Massnahmen getroffen werden, um unzutreffende oder unvollständige Daten zu berichtigen oder zu vernichten.

10. Datensicherheit

10.1 Für das Unternehmen ist von grosser Bedeutung, dass die Sicherheit der Daten jederzeit gewährleistet ist. Vor diesem Hintergrund sind die Personendaten durch technische und organisatorische Massnahmen u.a. gegen Verlust, gegen unbefugten Zugriff und vor anderen Gefahren zu schützen.

10.2 Für die einzelnen Vorgänge der Datenbearbeitung sind die konkreten Schutzmassnahmen zu dokumentieren und auf ihre Angemessenheit zu überprüfen.

10.3 Die IT-Abteilung kann weitergehende Vorgaben im Interesse der Datensicherheit erlassen, insbesondere in Bezug auf die Nutzung von IT-Systemen im Unternehmen.

11. Einwilligung und Widerspruch

11.1 Eine Einwilligung der betroffenen Person zur Datenbearbeitung durch ein Unternehmen ist grundsätzlich nicht erforderlich, auch nicht bei besonders schützenswerten Personendaten.

11.2 Widerspricht die betroffene Person hingegen einer Datenbearbeitung ausdrücklich, ist diese nur gerechtfertigt, wenn überwiegende Interessen des Verantwortlichen oder eine gesetzliche Grundlage vorliegen.

12. Informationspflicht

12.1 Betroffene Personen müssen möglichst vorgängig informiert werden, zu welchem Zweck Personendaten über sie erhoben und bearbeitet werden. Werden die Daten nicht direkt bei der betroffenen Person beschafft, wird diese innert eines Monats nach Erhalt der Daten informiert.

12.2 Macht die betroffene Person ihre Personendaten dem Verantwortlichen von sich aus zugänglich, gilt diese als informiert.

12.3 Wenn sich der Zweck der Datenbearbeitung ändert, müssen bereits informierte Personen erneut informiert werden.

13. Auftragsbearbeitung

13.1 Wenn Dienstleister des Unternehmens in dessen Auftrag Personendaten verarbeiten (sog. Auftragsbearbeiter), ist zu beachten, dass die gleichen Sorgfaltsanforderungen wie beim verantwortlichen Unternehmen auch für den Auftragsbearbeiter gelten. Insbesondere sind die Zweckbindung und Datensicherheit vertraglich sicherzustellen.

14. Übermittlung von Personendaten ins Ausland

14.1 Die Übermittlung von Personendaten ins Ausland ist nur in Staaten zulässig, in denen durch den Bundesrat ein ähnlich hohes Datenschutzniveau festgestellt wurde, wie in der Schweiz. Eine Einhaltung des Schweizer Datenschutzstandards kann zudem unter anderem durch den Abschluss zusätzlicher vertraglicher Vereinbarungen erreicht werden.

IV. Innerbetriebliche Prozesse

15. Anforderungen an Mitarbeiter

15.1 Alle Mitarbeiter des Unternehmens sind dem Datenschutz verpflichtet. Sie werden namentlich darüber informiert, dass es untersagt ist, Personendaten für private Zwecke zu nutzen, an Unbefugte zu übermitteln oder sie Unbefugten zugänglich zu machen. Die Pflicht zur Wahrung der Vertraulichkeit gilt über das Ende der Anstellung hinaus.

15.2 Auch innerhalb des Unternehmens ist darauf zu achten, dass nur die Mitarbeiter Zugriff auf Personendaten erhalten, die sie zur Erledigung ihrer Aufgaben für das Unternehmen benötigen.

15.3 Alle Mitarbeiter sollen zu Beginn ihrer Anstellung und nachfolgend regelmässig in Datenschutzthemen geschult und sensibilisiert werden.

16. Verzeichnis der Bearbeitungstätigkeiten

16.1 Das Unternehmen führt ein Verzeichnis der Bearbeitungstätigkeiten im Zusammenhang mit Personendaten. Darin müssen festgehalten werden: Identität des Verantwortlichen bzw. des Auftragsbearbeiters, Bearbeitungszweck, Beschreibung der Kategorien betroffener Personen und der Kategorien bearbeiteter Personendaten, Kategorien der Empfängerinnen und Empfänger, Aufbewahrungsdauer oder Kriterien zu deren Festlegung, wenn möglich Beschreibung der Massnahmen zur Datensicherheit sowie allfällige Zielstaaten, sollten die Daten ins Ausland gehen. Das Verzeichnis sollte stets aktuell sein und einen Überblick über die datenschutzrelevanten Aktivitäten im Unternehmen verschaffen.

17. Datenschutz durch Technik, datenschutzfreundliche Voreinstellungen sowie Datenschutz-Folgeabschätzung

17.1 Zur Bearbeitung von Personendaten genutzte Systeme sind von Anfang an so zu gestalten, dass der Datenschutz eingehalten werden kann. Die technischen und organisatorischen Massnahmen müssen insbesondere dem Stand der Technik, der Art und dem Umfang der Datenbearbeitung sowie dem Risiko, das die Bearbeitung für die Persönlichkeit oder die Grundrechte der betroffenen Personen mit sich bringt, angemessen sein (Privacy by Design).

17.2 Die Verantwortlichen haben die Standardeinstellung am Gerät bzw. an der Software so zu wählen, dass die Bearbeitung der Personendaten auf das für den Verwendungszweck nötige Mindestmass beschränkt ist, soweit die betroffene Person nicht etwas anderes bestimmt. Dies betrifft bspw. den Akzept von Cookies auf der Website.

17.3 Namentlich wenn eine geplante Datenschutzbearbeitung ein hohes Risiko für die Persönlichkeit und die Grundrechte betroffener Personen birgt, ist eine Datenschutz-Folgeabschätzung (DSFA) vorzunehmen und zu dokumentieren.

17.4 […]

V. Rechte der betroffenen Personen

18. Auskunftsrecht

18.1 Auf Anfrage ist einer betroffenen Person mitzuteilen, ob von dem Unternehmen Personendaten über sie bearbeitet werden. Sofern dies der Fall ist, hat die betroffene Person einen

Anspruch auf Auskunft über die entsprechenden Personendaten. Beim Auskunftsrecht geht es darum, in Erfahrung zu bringen, ob Personendaten bearbeitet werden und wenn ja, welche, sodass die betroffene Person ihre weiteren Rechte geltend machen kann. Dazu gehören neben den bearbeiteten Personendaten als solche Angaben zur Identität des Verantwortlichen, zum Bearbeitungszweck, zur Aufbewahrungsdauer, zur Datenherkunft und gegebenenfalls Informationen über automatisierte Einzelentscheide und die Empfänger (auch als Kategorien).

18.2 Bei der Auskunftserteilung ist sicherzustellen, dass die Identität der betroffenen Person verifiziert wird. Weiter ist zu beachten, dass im Rahmen der Auskunftserteilung keine Personendaten Dritter offenbart werden. Die Auskunft ist in der Regel kostenlos und innert 30 Tagen zu erteilen.

19. Datenportabilität / Recht auf Datenherausgabe und Datenübertragung

19.1 Betroffene Personen können ihre Daten, die sie dem Unternehmen bekannt gegeben haben, in einem gängigen elektronischen Format herausverlangen, wenn die Daten automatisiert bearbeitet werden und die betroffene Person zur Bearbeitung eingewilligt hat oder die Bearbeitung im Rahmen eines entsprechenden Vertrags erfolgt.

20. Recht auf Berichtigung

20.1 Eine betroffene Person kann nach Art. 32 Abs. 1 DSG verlangen, dass unrichtige Personendaten berichtigt werden.

21. Recht auf Datenlöschung

21.1 Wenn Personendaten entgegen der ausdrücklichen Willenserklärung der betroffenen Person bearbeitet werden und keine gesetzliche Grundlage und kein überwiegendes privates Interesse Dritter besteht, kann die betroffene Person die Löschung ihrer Personendaten verlangen.

[…]

VI. Zuständigkeit

22. Verantwortung

22.1 In erster Linie sind diejenigen Mitarbeiter für die Einhaltung der Vorgaben dieser Datenschutzrichtlinie verantwortlich, die jeweils mit der Datenbearbeitung betraut sind.

22.2 Alle Mitarbeiter des Unternehmens haben auf die Einhaltung dieser Datenschutzrichtlinie zu achten und auf diese Weise dazu beizutragen, dass in dem gesamten Unternehmen einheitlich hohe Datenschutzstandards etabliert werden.

22.3 Werden gesetzliche datenschutzrechtliche Pflichten verletzt, drohen den Fehlbaren strafrechtliche (Busse bis CHF 250'000.-) und dem Unternehmen zivilrechtliche (bis hin zu Schadenersatz) Konsequenzen sowie Reputationsschäden. Strafrechtlich verantwortlich ist in erster Linie die natürliche Person, d.h. der vorsätzlich fehlbare Mitarbeiter. Datenschutzverletzungen können auch unternehmensinterne disziplinarische Konsequenzen haben.

22.4 […]

23. Meldung von Verstössen und Zusammenarbeit mit Aufsichtsbehörden

23.1 Die Mitarbeiter haben dem Vorgesetzten bzw. dem Datenschutzbeauftragten unverzüglich Bericht zu erstatten, wenn sie Kenntnis von einem Verstoss gegen diese Datenschutzrichtlinie oder gesetzliche Bestimmungen haben, die sich auf den Schutz personenbezogener Daten beziehen.

23.2 Verletzungen der Daten*sicherheit* (z.B. Offenlegung für Unbefugte, Datenverlust, Cyberangriff etc.), die für die Betroffenen zu einem hohen Risiko für ihre Persönlichkeit oder ihre Grundrechte führen, müssen vom Unternehmen dem EDÖB «so rasch als möglich», also zeitnah, gemeldet werden.

23.3 […]

VII. Weitere Bestimmungen

24. Publizität

24.1 Diese Unternehmensrichtlinie ist allen Mitarbeitern des Unternehmens in geeigneter Weise zugänglich zu machen, [insbesondere über das Intranet].

24.2 Eine allgemeine Veröffentlichung dieser Datenschutzrichtlinie ist nicht vorgesehen.

25. Änderungen

25.1 Das Unternehmen behält sich das Recht vor, diese Datenschutzrichtlinie bei Bedarf zu ändern. Eine Änderung kann insbesondere erforderlich werden, um gesetzlichen Vorgaben, Forderungen der Aufsichtsbehörden oder unternehmensinternen Verfahren zu entsprechen.

25.2 In regelmässigen Abständen soll auch geprüft werden, inwieweit technologische Veränderungen eine Anpassung dieser Unternehmensrichtlinie erforderlich machen.

26. […]