

Gültigkeit/Verteiler:

x													
Alle	GF	Med.	MSD	PD	PT	Phy	Ergo	VwE	Kü	Se	HT	Fa	Re

Datenschutzrichtlinie

Unser Unternehmen *HolsingVital* beachtet gesetzliche Vorschriften und achtet auf die Wahrung unserer wie auch der Betriebs- und Geschäftsgeheimnisse unserer Geschäftspartner. Das schließt alle Formen der bei uns praktizierten oder durch Outsourcing bei Dienstleistern durchgeführten Datenverarbeitung ein. Vor diesem Hintergrund ergeht folgende Richtlinie:

I. Grundsätze

Vermutete oder erwiesene Verstöße gegen Datensicherheit und Datenschutz („Datenpannen“) sind in unserem Unternehmen meldepflichtig gemäß den nachfolgenden Bestimmungen.

Die Meldepflicht wird für denjenigen Verantwortlichen ausgelöst, der in seinem Arbeitsbereich auf eine vermutete oder erwiesene „Datenpanne“ stößt oder hingewiesen wird. Mitarbeiter melden derartige Beobachtungen dem Vorgesetzten, der nach den nachfolgenden Bestimmungen verfährt.

Die hier festgelegte Meldepflicht bezieht sich auf interne Informationspflichten und deren Wege; inwieweit eine Offenlegung nach außen geboten ist, obliegt dem in Ziffer V bestellten Entscheidungsgremium.

II. Datenpannen

Als „Datenpannen“ werden alle schädlichen Ereignisse bei der Datenverarbeitung angesehen, die vom Datenschutzrecht geschützte personenbezogene Daten sowie solche Daten betreffen, die im Sinne unseres Unternehmens oder im Hinblick auf die Haftung gegenüber unseren Geschäftspartnern als schutzwürdig anzusehen sind (eigene und fremde Betriebs- und Geschäftsgeheimnisse).

Namentlich sind als „Datenpannen“ definiert:

1. Formen bewusster oder unbewusster unbefugter oder rechtswidriger Verarbeitung schutzwürdiger Daten.
2. Unbefugte Aktivitäten zur Umgehung von Sicherheitsvorkehrungen, die dem Schutz schutzwürdiger Daten dienen.
3. Angriffe auf die IT-Infrastruktur des Unternehmens, die vermutlich oder offensichtlich erfolgreich waren.

Gültigkeit/Verteiler:

x													
Alle	GF	Med.	MSD	PD	PT	Phy	Ergo	VwE	Kü	Se	HT	Fa	Re

Unter „Verarbeitung von Daten“ ist zu verstehen:

1. Erhebung,
2. Speicherung,
3. Veränderung,
4. Abruf,
5. Einsicht,
6. Löschung,
7. Nutzung von Daten.

III. Wahrnehmung von Datenpannen

Datenpannen können unterschiedlich wahrgenommen werden. Zu unterscheiden ist zwischen „intern“ und „extern“:

Von innen:

1. Alarme aufgrund von Warnmechanismen
2. Anomalien in der Verarbeitung schutzwürdiger Daten
3. Erkenntnisse aus dem Incident Handling sowie dem Problem Management
4. Erkenntnisse aus Prüfungen
5. Erkenntnisse aus Mitarbeitergesprächen

Von außen:

1. Hinweise Dritter
2. Medienberichte
3. Anzeigen

IV. Berichtswege und interne Abstimmung

Mitarbeiter, die eine tatsächliche oder vermutete Datenpanne wahrnehmen, informieren unverzüglich

- ihren Vorgesetzten
- und gleichzeitig den betrieblichen Datenschutzbeauftragten.

Ist eine dieser beiden Personen abwesend, handelt der jeweils andere allein; im Regelfall unternehmen sie gemeinsam folgende Schritte:

Anfertigen eines als „vertraulich“ gekennzeichneten Protokolls, das die Erkenntnisse des meldenden Mitarbeiters beschreibt.

Gültigkeit/Verteiler:

x													
Alle	GF	Med.	MSD	PD	PT	Phy	Ergo	VwE	Kü	Se	HT	Fa	Re

Verteilung des Protokolls an „Pflichtempfänger“:

1. Geschäftsführung,
2. Leiter der Abteilungen, welche die Datenpanne berührt,
3. IT-Sicherheitsbeauftragter,

Verteilung des Protokolls „fallorientierte Empfänger“:

1. Einkauf, soweit Fremdfirmen betroffen sind oder sein können,
2. Vertrieb, soweit Vertriebsstrukturen berührt sind oder sein können,
3. Personalleitung, soweit es Hinweise auf Fehlverhalten von Beschäftigten gibt (die Personalleitung informiert seinerseits den Betriebsrat, sofern es sich um Tatbestände der Mitbestimmung nach dem Betriebsverfassungsgesetz handelt).

V. Klärung des Sachverhalts und Aktionen

Über das weitere Vorgehen entscheidet die Geschäftsführung nach Anhörung des betrieblichen Datenschutzbeauftragten und der Leiter der Abteilungen, die von der Datenpanne berührt sind.

Zu klären ist, inwieweit

- Strafanzeige zu erstatten ist
- personelle Maßnahmen zu ergreifen sind
- eine Zusammenarbeit mit einem betroffenen Unternehmen zu beenden ist
- Haftungsansprüche geltend gemacht werden können,
- eine Benachrichtigung der Aufsichtsbehörde für den Datenschutz erforderlich ist
- von der Datenpanne betroffene Personen einzeln zu benachrichtigen sind,
- wahlweise eine allgemeine Anzeige in nach § 42a BDSG vorgeschriebenen Zeitungsannoncen durchzuführen ist,
- Änderungen in bestehenden Verfahren vorzunehmen sind, um Wiederholungen zu vermeiden.

Das Ergebnis wird protokolliert und steht neben den unter IV genannten „Empfängern“ dem Wirtschaftsprüfer zur Verfügung.

VI. Hinweise

Alle Vorkommnisse werden intern und vertraulich behandelt. Über eine Veröffentlichungspflicht nach § 42a BDSG entscheidet eine Prüfung durch die Geschäftsführung im Benehmen mit dem betrieblichen Datenschutzbeauftragten.

Beschäftigte, die vermutete oder tatsächliche Datenpannen wahrgenommen und gemeldet haben, erleiden keinerlei Nachteile aus der Tatsache, dass sie gemäß dieser Richtlinie gehandelt haben.