KICKSCALE

ANLAGE 1

zur Informationssicherheitsrichtlinie für Kickscale

VORGEHEN BEI EINEM DATENSCHUTZVORFALL

1. Allgemeines

Die DSGVO definiert einen Datenschutzvorfall ("**Data Breach**") gemäß Art 4 Z 12 DSGVO als eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von bzw zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.

Ein Data Breach ist daher beispielsweise ein Vorfall, durch den Unbefugten der Zugriff auf Daten ermöglicht wird (z.B. Verlust eines Datenträgers, Hackerangriff, Weiterleitung von E-Mails an einen falschen Empfänger). Dadurch kann den betroffenen Personen ein physischer, materieller oder immaterieller Schaden entstehen. Folgen eines Data Breaches können neben dem Verlust der Kontrolle über personenbezogenen Daten auch Identitätsdiebstahl oder –betrug, finanzielle Verluste, Rufschädigung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile sein.

Sicherheitsverletzungen können grundsätzlich in drei Kategorien eingeteilt werden:

- **Verletzung der Vertraulichkeit** ("*Confidentiality Breach*"): Unbefugte oder versehentliche Offenlegung von oder Zugang zu personenbezogenen Daten;
- **Verletzung der Integrität** ("*Integrity Breach*"): Unbefugte oder versehentliche Änderung personenbezogener Daten
- **Verletzung der Verfügbarkeit** ("*Availability Breach*"): Unbefugter oder versehentlicher Verlust des Zugriffs auf personenbezogene Daten oder deren Vernichtung.

Ein Datenschutzvorfall kann auch mehrere dieser Kategorien betreffen.

Die DSGVO sieht strenge Fristen für die Meldung eines Datenschutzvorfalls vor. In manchen Fällen müssen sowohl die Aufsichtsbehörde als auch die Betroffenen unverzüglich, aber spätestens binnen 72 Stunden, nachdem der Datenschutzvorfall bekannt wird, über einen Data Breach informiert werden (Art 33 und 34 DSGVO).

Unabhängig von der Meldepflicht muss der Verantwortliche jeden Datenschutzvorfall einschließlich aller im Zusammenhang mit diesem Vorfall stehenden Fakten, deren Auswirkungen und die ergriffenen Abhilfemaßnahmen dokumentieren (Art 33 Abs 5 DSGVO).

2. Informationsfluss bei Kickscale

Damit allfällige Sicherheitsvorfälle nicht zu gravierenden Datenschutzverletzungen oder ernsten Sicherheitsproblemen werden, müssen alle Auffälligkeiten, mögliche oder tatsächliche Gefahren für die Datensicherheit sowie befürchtete oder tatsächliche Datenschutzvorfälle unverzüglich an den Datenschutzbeauftragten gemeldet werden. Sofern dieser nicht unverzüglich erreicht werden kann, muss eine (andere) Person der Geschäftsführung informiert werden.

Kontaktdaten des Datenschutzbeauftragten:	
Name:	Fabian Riedlsperger
E-Mail:	fabian.riedlsperger@kickscale.com
Tel.Nr.:	+436766232723

Für Meldungen an den Datenschutzbeauftragten steht das **Data Breach Meldeformular in Appendix A** zur Verfügung. Dieses Meldeformular ermöglicht eine schnelle Ersteinschätzung, ob der Sicherheitsvorfall ein meldepflichtiger Datenschutzvorfall ist. Dazu sind insbesondere folgende Informationen bereitzustellen:

- Wer ist/war betroffen?
  (zB Kunden, Mitarbeiter, sonstige Dritte)
- Was ist geschehen?
  (zB E-Mail an den falschen Empfänger gesendet)
- Welche personenbezogenen Daten sind betroffen? Sind sensible Daten iSd Art 9 DSGVO umfasst?
- Unter welchen Umständen ist es zu dem Vorfall gekommen?
  (zB menschliches Fehlverhalten, unbewusste Änderung von Kontaktdaten)
- Wie haben Sie reagiert?
  (zB allfällige Rückmeldungen an falsche Empfänger)
- Wann und wie haben Sie Kenntnis von dem Vorfall erlangt?
  (zB durch Mitteilung eines Dritten, Vorfall selbst erkannt, etc)

Grundsätzlich gilt: Je mehr Informationen über den möglichen Data Breach vorliegen, desto schneller und zielgerichteter kann die Prüfung erfolgen. Wir bitten Sie daher, alle Auffälligkeiten oder Unregelmäßigkeiten zu melden, auch wenn Sie befürchten, selbst falsch reagiert zu haben. Ihre Meldung wird vertraulich behandelt.

3. Risikoabschätzung und Meldung

Nach Erhalt einer Meldung wird der Datenschutzbeauftragte das Risiko bewerten und den Vorfall in die folgenden Kategorien einteilen. Je nach Risikokategorie leitet der Datenschutzbeauftragte die folgenden Schritte ein:

Klassifizierung		Folge
	Kein Risiko	Der Datenschutzvorfall führt voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen ➔ Interne Dokumentation des Vorfalls (**Appendix B**)
	Risiko	Der Datenschutzvorfall führt voraussichtlich zu einem Risiko für die Rechte und Freiheiten natürlicher Personen ➔ Meldung an die Aufsichtsbehörde ➔ Interne Dokumentation des Vorfalls
	Hohes Risiko	Der Datenschutzvorfall führt voraussichtlich zu einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen ➔ Meldung an die Aufsichtsbehörde ➔ Benachrichtigung der Betroffenen ➔ Interne Dokumentation des Vorfalls

Bei der Beurteilung des Risikos sind sowohl die Marktpraxis als auch die Guidelines des Europäischen Datenschutzausschusses (Guidelines 9/22 on personal data breach notification under GDPR) zu berücksichtigen.

3.1. Meldung an die Datenschutzbehörde

Wenn die Datenschutzverletzung voraussichtlich zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt, muss der Vorfall gemäß Art 33 DSGVO unverzüglich, spätestens aber **binnen 72 Stunden nachdem der Data Breach bekannt geworden ist** an die Aufsichtsbehörde gemeldet werden. Sofern die Meldung nicht innerhalb dieses Zeitraums erfolgten kann, so muss in der Meldung eine Begründung für die Verzögerung angeführt werden.

Die Meldung an die Aufsichtsbehörde muss folgende Informationen enthalten:

- Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten
- Ungefähre Anzahl der betroffenen Personen und Datensätze
- Beschreibung der wahrscheinlichen Folgen der Verletzung
- Beschreibung der ergriffenen und vorgeschlagenen Maßnahmen zur Abmilderung möglicher, nachteiliger Auswirkungen

Zur Meldung an die Behörde kann das Meldeformular der DSB (https://dsb.gv.at/eingabe-an-die-dsb/-meldung-data-breach) verwendet werden.

Wenn die betroffene Verarbeitungstätigkeit im Rahmen der Auftragsverarbeitung durchgeführt wird, so ist der jeweilige Verantwortliche unverzüglich zu informieren.

Zusätzlich muss der Data Breach samt damit im Zusammenhang stehenden Fakten, Auswirkungen und ergriffenen Abhilfemaßnahmen gemäß Art 33 Abs 5 DSGVO **dokumentiert** werden. Diese Dokumentation muss der Aufsichtsbehörde die Überprüfung des Vorfalls ermöglichen.

3.2. Benachrichtigung der betroffenen Personen

Wenn die Datenschutzverletzung voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge hat, so muss der Verantwortliche nicht nur die zuständige Aufsichtsbehörde, sondern auch die Betroffenen gemäß § 34 DSGVO über den Vorfall informieren. Diese Meldung hat die folgenden Informationen in klarer und einfacher Sprache zu enthalten:

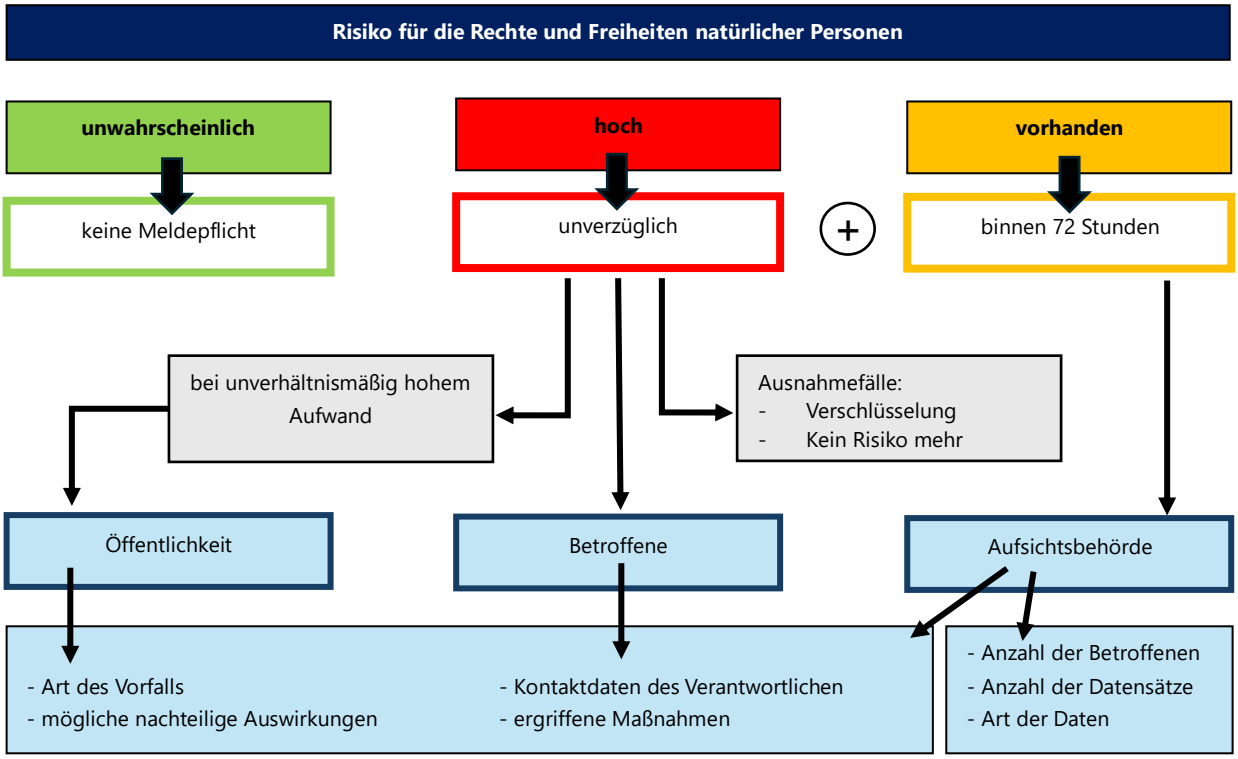
- Art des Datenschutzvorfalls
- Beschreibung der wahrscheinlichen Folgen des Datenschutzvorfalls
- Beschreibung der ergriffenen und vorgeschlagenen Maßnahmen zur Abmilderung möglicher, nachteiliger Auswirkungen
- Namen und Kontaktdaten des für die Verarbeitung personenbezogener Daten Verantwortlichen

In bestimmten Fällen ist eine Benachrichtigung an die betroffenen Personen nicht erforderlich:

- Der Verantwortliche hat geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen, sodass die personenbezogenen Daten für Unbefugte unzugänglich sind (zB durch Verschlüsselung);

- Der Verantwortliche hat durch nachfolgende Maßnahmen sichergestellt, dass das hohe Risiko nicht mehr besteht.

Sofern die Benachrichtigung der Betroffenen mit einem unverhältnismäßigen Aufwand verbunden wäre, so kann statt der individuellen Benachrichtigung eine öffentliche Bekanntgabe oder eine ähnliche Maßnahme erfolgen, durch die die betroffenen Personen vergleichbar wirksam informiert werden.


Risiko für die Rechte und Freiheiten natürlicher Personen
unwahrscheinlich
hoch
vorhanden
keine Meldepflicht
unverzüglich
+
binnen 72 Stunden
bei unverhältnismäßig hohem Aufwand
Ausnahmefälle:
- Verschlüsselung
- Kein Risiko mehr
Öffentlichkeit
Betroffene
Aufsichtsbehörde
- Art des Vorfalls
- mögliche nachteilige Auswirkungen
- Kontaktdaten des Verantwortlichen
- ergriffene Maßnahmen
- Anzahl der Betroffenen
- Anzahl der Datensätze
- Art der Daten

Appendix A

Data Breach Meldeformular

Dieses Meldeformular ermöglicht eine schnelle Ersteinschätzung, ob der Sicherheitsvorfall ein meldepflichtiger Datenschutzvorfall ist. Bitte übermitteln Sie dieses Meldeformular so schnell und so vollständig als möglich an den Datenschutzbeauftragten:

Kontaktdaten des Datenschutzbeauftragten:

Name: Fabian Riedlsperger

E-Mail: fabian.riedlsperger@kickscale.com

Eine unverzügliche Meldung an den Datenschutzbeauftragen ist wichtig, weil Kickscale einen meldepflichtigen Vorfall **binnen 72 Stunden** an die Aufsichtsbehörde melden muss. Im Falle einer Verzögerung können erhebliche Strafen verhängt werden!

1) Angaben zum Zeitpunkt des Vorfalls:

Wann ist Ihnen der Vorfall erstmals bekannt geworden? _____

Wer hat den Vorfall bemerkt? _____

Ist Ihnen bekannt, wann der Vorfall stattgefunden bzw begonnen hat?

□ Nein □ Ja, am _____

Hält der Zustand des Vorfalls nach wie vor an?

□ Nein □ Ja

Besteht ein Risiko, dass sich der Vorfall wiederholt?

□ Nein □ Ja

2) Art des Vorfalls:

Bitte wählen Sie die Art des Datenschutzvorfalls aus (Mehrfachauswahl ist möglich)

- □ Personenbezogene Daten wurden einer unbefugten Person **offengelegt**
  (zB Dokumente oder Datenträger wurden gestohlen oder an öffentlichen Orten vergessen)

- □ Unbefugte Personen haben **unbefugten Zugang** zu personenbezogenen Daten erhalten
  (zB Hacking, Phishing-Attacken, Missbrauch von Zugriffsrechten durch eigene Mitarbeiter)

- □ Personenbezogene Daten wurden unberechtigterweise **an Dritte übermittelt**
  (zB E-Mail wurde an einen falschen Empfänger gesendet)

- □ Personenbezogene Daten sind **verloren** gegangen
  (zB Verlust von Dokumenten, Datenträgern, Hardware, etc)

- □ Personenbezogene Daten wurden **inhaltlich manipuliert** oder **verfälscht**
  (zB unzulässige Änderung des Inhalts)

- □ Der **Zugang** zu personenbezogenen Daten ist **nicht mehr möglich**
  (zB Systemfehler oder Verlust von Daten ohne Möglichkeit der Widerherstellung)

- □ Andere Vorfälle:
  _____
  _____
  _____
  _____
  _____
  _____

Der Vorfall ereignete sich:

□ vorsätzlich □ zufällig □ keine Angabe

Bitte beschreiben Sie, **wie und warum** sich der Vorfall ereignet hat:

Wie haben Sie **reagiert**?

3) Betroffene Daten

Der Vorfall betrifft die folgenden **Arten von personenbezogenen Daten** (Mehrfachauswahl möglich):

□ Namen
□ Geburtsdaten
□ Adressdaten
□ (Elektronische) Kontaktdaten
□ Elektronische Identifikationsdaten
□ Standort oder Bewegungsdaten
□ Zugangsdaten (Passwörter)
□ Vertragsdaten
□ Kontoinformationen
□ Andere: _____

Der Vorfall betrifft die folgenden **sensiblen Daten** (Mehrfachauswahl möglich)

□ Gesundheitsdaten
□ Genetische Daten
□ Biometrische Daten
□ Daten über die sexuelle Orientierung
□ Ethnische Herkunft
□ Politische Ansichten
□ Religion oder Weltanschauung
□ Gewerkschaftszugehörigkeit

□ Es sind keine sensiblen Daten betroffen

4) Angaben zu den Betroffenen

Der Vorfall betrifft die folgenden Gruppen von Betroffenen (Mehrfachauswahl möglich):

□ Mitarbeiter
□ (potentielle) Kunden
□ Dienstleister
□ Minderjährige oder geistig beeinträchtigte Personen
□ andere: _____

Wie viele Personen sind voraussichtlich vom Vorfall betroffen?

□ 1 bis 9
□ 10 bis 490
□ 500 bis 2.000
□ über 2.000

Wie viele Datensätze sind voraussichtlich betroffen?

□ unter 1.000
□ unter 10.000
□ unter 50.000
□ unter 100.000
□ über 100.000

Datum: _____

Appendix B
Dokumentation eines Data Breach

[**Titel**]

Datum und Zeit des Datenschutzvorfalls: [●], um [●] Uhr

Datum des Bekanntwerdens des Datenschutzvorfalls: [●], um [●] Uhr

Interne Meldung des Datenschutzvorfalls: [Name/Speicherpfad/Beilage des Dokuments der internen Meldung]

Beschreibung des Datenschutzvorfalls:

Es handelt sich um folgende Art der Verletzung des Schutzes personenbezogener Daten:

- □ Verletzung der Vertraulichkeit
- □ Verletzung der Integrität
- □ Verletzung der Verfügbarkeit

Betroffene Personen:

Kategorien der betroffenen Personen: [●]

Ungefähre Anzahl der betroffenen Personen: [●]

Betroffene Daten:

Kategorien der betroffenen Daten: [●]

Ungefähre Anzahl der betroffenen Datensätze: [●]

Folgende **Maßnahmen wurden zur Behebung/Abmilderung** der Verletzung des Schutzes personenbezogener Daten ergriffen:

Der Datenschutzvorfall führt voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen, weil:

Erstellt von [Name]

Datum [•]