Technische und organisatorische Maßnahmen nach Art. 32 DS-GVO

Kicktipp hat unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen getroffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Die Verarbeitung von Daten findet dabei an verschiedenen Orten statt, die nachfolgenden beschrieben sind. Soweit für diese Orte unterschiedliche Schutzmaßnahmen gelten, wird dies bei den jeweiligen Maßnahmen erwähnt.

Rechenzentrum

Hier findet die hauptsächliche Verarbeitung bei Kicktipp statt. Alle Vorgänge, die Tipper oder Spielleiter vornehmen werden automatisiert hier durchgeführt. Das Rechenzentrum ist räumlich vom Kicktipp Büro getrennt. Das Rechenzentrum wird von der Hetzner Online GmbH betrieben. Die Hetzner Online GmbH ist Auftragsverarbeiter der Kicktipp GmbH.

Kicktipp

Zur Administration und Wartung von Systemen und zur Beantwortung von Serviceanfragen wird auf die Systeme im Rechenzentrum aus dem Kicktipp Büro zugegriffen. Der Zugriff kann auch aus dem mobilen Büro bzw. Home-Office erfolgen.

1. Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Rechenzentrum

- Elektronisches Zutrittskontrollsystem mit Protokollierung
- Hochsicherheitszaun
- Dokumentierte Schlüsselvergabe an Mitarbeiter
- Richtlinien zur Begleitung und Kennzeichnung von Gästen im Gebäude
- 24/7 personelle Besetzung der Rechenzentren
- Videoüberwachung an den Ein- und Ausgängen, Sicherheitsschleusen und Serverräumen
- Der Zutritt für betriebsfremde Personen nur in Begleitung eines Mitarbeiters.

Kicktipp

- Manuelles Schließsystem
- Klingelanlage mit Kamera
- Der Zutritt für betriebsfremde Personen erfolgt nur in Begleitung eines Mitarbeiters
- Im mobilen Büro findet naturgemäß keine Zutrittskontrolle statt. Jedes Endgerät wird selbst durch Zugangskontrollen geschützt.

2. Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Rechenzentrum

- Zugriff auf Systeme bei erstmaliger Inbetriebnahme erfolgt mittels Public-Privat-Key-Verfahren. Der Private-Key ist ausschließlich auf einem externen Security Token gespeichert und kann nicht ausgelesen werden. Er ist zusätzlich mit einem Pin Code gesichert.
- Der Zugriff auf die Administrationsoberfläche des Rechenzentrums erfolgt mittels Zwei-Faktor-Authentifizierung.
- Alle Systeme von Kicktipp im Rechenzentrum sind dedizierte Server.
- Alle Systeme werden automatisiert installiert, um eine einheitliche Zugangskontrolle zu gewährleisten.
- Jedes System ist mit einer Firewall ausgestattet. Nur benötigte Ports und Dienste sind freigeschaltet.
- Sicherheitsupdates werden unmittelbar nach Mitteilung durch das Betriebssystem eingespielt.

Kicktipp

- Datenträger in Desktops, Laptops oder Smartphones sind verschlüsselt. Jedes Gerät ist einem Mitarbeiter zugeordnet. Nur dieser kennt die Passphrase zur Entschlüsselung.
- USB-Sticks werden verschlüsselt. Auf die Verschlüsselung wird verzichtet, wenn der USB-Stick ausschließlich öffentlich zugängliche Software enthält (zb Installationsstick)
- Verwaltung von Benutzerberechtigung
- Jeder Mitarbeiter hat ein sicheres und nur ihm bekanntes Passwort zu verwenden.
- Es wird bei allen Desktop und Laptops Linux als Systemsoftware eingesetzt. Bei Smartphones kommt Stock-Android oder iOS zum Einsatz.
- Testgeräte mit Windows verarbeiten keinerlei Daten, sondern dienen nur zum Testen der Funktionalität auf Windowsgeräten
- Sicherheitsupdates werden unmittelbar nach Mitteilung durch das Betriebssystem eingespielt.

3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Rechenzentrum

- Bei internen Verwaltungssystemen im Rechenzentrum werden regelmäßige Sicherheitsupdates (nach dem jeweiligen Stand der Technik) durchgeführt.
- Es gibt ein revisionssicheres, verbindliches Berechtigungsvergabeverfahren für Mitarbeiter im Rechenzentrum.

Kicktipp

- Der Zugriff auf Betriebssystemebene erfolgt ausschließlich mittels Public-Privat-Key-Verfahren. Der Private-Key ist ausschließlich auf einem externen Security Token gespeichert und kann nicht ausgelesen werden. Er ist zusätzlich mit einem Pin Code gesichert.
- Für Servicemitarbeiter erfolgt der Zugriff über ein definiertes Webinterface mit Hilfe von Benutzerkennung und Passwort.
- Die Anzahl der Mitarbeiter mit Zugriff auf Betriebssystemebene ist auf drei beschränkt.

4. Datenträgerkontrolle

Rechenzentrum

- Festplatten werden nach Kündigung mit einem definierten Verfahren mehrfach überschrieben (gelöscht). Nach Überprüfung werden die Festplatten wieder eingesetzt.
- Defekte Festplatten, die nicht sicher gelöscht werden können,werden direkt im Rechenzentrum zerstört (geschreddert)

Kicktipp

- Datenträger werden vor der Entsorgung überschrieben und gelöscht.

5. Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Rechenzentrum

- Daten aus verschiedenen Tippspielen werden logisch getrennt voneinander gespeichert (Mandantenfähigkeit)
- Im Rechenzentrum laufen ausschließlich Produktivsysteme. Diese sind von Testsystemen physikalisch getrennt.

Kicktipp

- Im Kicktipp Büro laufen ausschließlich Testsysteme. Diese sind vom Produktivsystem physikalisch getrennt.

6. Pseudonymisierung

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen.

- Passwörter werden ausschließlich verschlüsselt gespeichert.
- Bei der Eingabe der E-Mail Adresse und des Tippernames entscheidet der Nutzer, ob er pseudonymisierte Daten einsetzt.
- Eine Weiterverarbeitung der Daten findet nur durch den Kunden/Spielleiter statt (Menüpunkt „Datenexport“). Der Kunde/Spielleiter entscheidet über eine anschließende Pseudonymisierung.
- Soweit ein Tippspiel die Eingabe weiterer Daten wie Adresse, Geburtsdatum etc. aufgrund der Einstellung des Spielleiters verlangt, wird von Kicktipp keine Pseudonymisierung vorgenommen. Für die weitere Pseudonymisierung ist auch hier der Kunde/Spielleiter verantwortlich.

7. Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Rechenzentrum

- Im Rechenzentrum kommunizieren die einzelnen dedizierten Server nur in einem privaten Netwzwerk.
- Datenverkehr über öffentliche Leitungen findet verschlüsselt statt

Kicktipp

- Datenverkehr über öffentliche Leitungen findet in der Regel verschlüsselt statt. Im Einzelfall kann es zu Ausnahmen kommen, wenn Webseiten nicht verschlüsselt angeboten werden.
- Der Versand von E-Mails erfolgt über eigene Mailserver direkt an den Mailserver des Kunden. Der Versand der Mails erfolgt verschlüsselt. (Transportverschlüsselung)

8. Eingangskontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- Die Eingabe der Daten erfolgt über den Kunden als Spielleiter oder Tipper selbst.

- Es findet eine Protokollierung der Zugriffe statt.

9. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Rechenzentrum

- Einsatz unterbrechungsfreier Stromversorgung, Netzersatzanlage.
- Dauerhaft aktiver DDoS-Schutz.
- Redundante Serversysteme
- Monitoring aller relevanten Server hinsichtlich Verfügbarkeit und Auslastung
- Einsatz von Festplattenspiegelung bei allen relevanten Servern
- Sachkundiger Einsatz von Schutzprogrammen (Firewalls, Verschlüsselungsprogramme)
- Backup- und Recovery-Konzept mit täglicher Sicherung aller relevanten Daten
- Vorhalten redundanter System für Ausfall und rasche Wiederherstellung
- Modernes Brandschutzsystem, siehe https://www.hetzner.com/de/unternehmen/rechenzentrum/

Kicktipp

- Es findet im Kicktipp Büro keine Speicherung oder Verarbeitung relevanter Daten statt.

10. Datenschutzmaßnahmen

Rechenzentrum

- Sicherheitszertifizierung des Rechenzentrums nach ISO 27001

Kicktipp

- Externer Datenschutzbeauftragter
- Jährliche Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen durch den externen Datenschutzbeauftragten
- Alle Mitarbeiter werden regelmäßig im Hinblick auf Datenschutz, Vertraulichkeit und Datengeheimnis geschult. Die Schulungsnachweise können über unsere Webseite eingesehen werden.
- Jeder Nutzer hat die Möglichkeit seine Daten vollständig zu löschen. Im Menüpunkt „Mein Profil“ findet sich der Link „Konto löschen“ mit genauen Anweisungen.

11. Incident-Response-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen.

- Einsatz eines Intrusion-Detection-Systems
- Soweit es zu einem Sicherheitsvorfall kommt, werden alle Betroffenen per E-Mail informiert.
- Bei einem Sicherheitsvorfall wird die zuständige Behörde unverzüglich informiert, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.
- Zusätzlich werden alle Sicherheitsvorfälle, Auszeiten und geplante Wartungsarbeiten auf unsere Seite Aktuelles veröffentlicht.

12. Datenschutzfreundliche Voreinstellungen

- Datenschutzfreundliche Voreinstellungen werden bei Softwareentwicklungen berücksichtigt. Jegliche Datenerhebung von Kicktipp selbst darf nur dem Zweck der Verbesserung des Tippspiels oder der Kommunikation im Tippspiel dienen.

- Soweit der Spielleiter zusätzliche Daten erhebt, obliegt dem Spielleiter die Einhaltung datenschutzfreundlicher Voreinstellung.

13. Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

- Alle Mitarbeiter werden in regelmäßigen Abständen im Datenschutzrecht unterwiesen und sie sind vertraut mit den Verfahrensanweisungen und Benutzerrichtlinien für die Datenverarbeitung im Auftrag, auch im Hinblick auf das Weisungsrecht des Auftraggebers.
- Die Auftragsverarbeitungsverträge enthalten detaillierte Angaben über Art und Umfang der beauftragten Verarbeitung und Nutzung personenbezogener Daten des Auftraggebers.
- Die Kicktipp GmbH hat einen externen Datenschutzbeauftragten bestellt. Dieser ist in die relevanten betrieblichen Prozesse eingebunden.
- Der Betreiber des Rechenzentrums ist die Hetzner Online GmbH. Der Betreiber wurde sorgfältig ausgewählt und steht seit vielen Jahren für hervorragende Qualität und Sicherheit.
  https://www.hetzner.com/de/unternehmen/ueber-uns

Das Dokument wird fortlaufend erweitert und aktualisiert. Die jeweils gültige Fassung finden Sie unter
https://www.kicktipp.de/download/datenschutz/

2021-06-28

Kicktipp GmbH
Janning Vygen
vygen@kicktipp.de