

## **Regelung zur Datenverarbeitung**

**Veszprém-Balaton 2023 Zrt.**

**(im Weiterem: der Verantwortliche oder die Organisation)**

**Bezüglich der durch sie verarbeiteten personenbezogenen Daten**

**Datenschutzbeauftragte: dr. Judit Bazsala**

**Vertreter des Verantwortlichen: Aliz Markovits geschäftsführende Direktorin**

## Inhaltsverzeichnis

1. PRÄAMBEL.....	4
2. ALLGEMEINE BESTIMMUNGEN.....	6
2.1. Zweck und Gültigkeit der Regelung.....	6
2.2. Grundbegriffe des Datenschutzes .....	6
3. METHODOLOGISCHE REGELN DER VERARBEITUNG PERSONENBEZOGENER DATEN .....	8
3.1. Grundsätze bezüglich der Verarbeitung personenbezogener Daten.....	8
3.2. Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten.....	9
4. BEI DER ORGANISATION STATTFINDENDE DATENVERARBEITUNGEN .....	10
4.1. Datenverarbeitung bezüglich der Gründung, Aufrechterhaltung und dem Beenden eines Arbeitsverhältnisses .....	10
4.2. Lohn- und Arbeitsverzeichnis .....	11
4.3. Arbeitsschutz, Brandschutz, Unfallschutz.....	12
4.4. Datenverarbeitung bezüglich der Firmenhandys der Arbeitnehmer:.....	12
4.5. Praktikanten.....	13
4.6. Datenverarbeitung bezüglich des Betreibens von Seiten der sozialen Medien.....	13
4.7. Datenverarbeitung bezüglich Marketing, Newsletter:.....	14
4.8. Datenverarbeitung bezüglich Bewerbungen.....	14
5. DATENSCHUTZSYSTEM DER ORGANISATION.....	15
5.1. Datenschutzorganisation innerhalb der Organisation.....	15
5.2. Regeln für Datensicherheit .....	17
6. VERLETZUNG DES SCHUTZES PERSONENBEZOGENER DATEN .....	19
6.1. Begriff eines Vorfalls der Verletzung des Schutzes personenbezogener Daten im Bereich Datenschutz.....	19
6.2. Handhabung eines Vorfalls der Verletzung des Schutzes personenbezogener Daten	19
6.3. Erfassen eines Vorfalls der Verletzung des Schutzes personenbezogener Daten .....	20
7. VORSTELLUNG DER FOLGENABSCHÄTZUNG FÜR DATENSCHUTZ, DER VORANGEHENDEN KONSULTATION UND DER INTERESSENABWÄGUNG .....	21
7.1. Datenschutz-Folgenabschätzung .....	21
7.2. Vorherige Konsultation .....	22
7.3. Interessenabwägung.....	22
8. GELTENDMACHUNG DER RECHTE DER BETROFFENEN.....	23
8.1. Übersichtliche Aufklärung, Kommunikation und Unterstützung der Ausübung der Rechte der Betroffenen.....	23
8.2. Zugriffsrecht der Betroffenen .....	24
8.3. Recht auf Berichtigung.....	25
8.4. Recht auf Datenlöschung .....	25

8.5. Recht auf Einschränkung der Verarbeitung .....	26
8.6. Recht auf Datenübertragbarkeit .....	26
8.7. Widerspruchsrecht .....	27
8.8. Automatisierte Entscheidungen im Einzelfall einschließlich Profiling.....	27
8.9. Recht auf Rechtsbehelf .....	28
9. SCHLUSSBESTIMMUNGEN .....	28
10. ANLAGEN.....	29

## **1. PRÄAMBEL**

Die Veszprém-Balaton 2023 Zrt. und ihre verbundenen Unternehmen (im Weiterem: die Organisation, die Organisationen) erstellen zum Erfassen ihrer internen Datenverarbeitungsprozesse und der Sicherstellung der Rechte der betroffenen Personen folgende Regelung zur Datenverarbeitung (im Weiterem: Regelung).

### **Angaben des Verantwortlichen:**

#### **Veszprém-Balaton 2023 geschlossen tätige Aktiengesellschaft**

Firmensitz: Veszprém 8200, Óváros tér 26.

Firmenregisternummer: 19-10-500277

E-Mail: info@veszprembalaton2023.hu

Telefon: 0688 794 028

### **Angaben der Auftragsverarbeiter:**

#### **Molnár és Társa Kft.**

Firmensitz: Balatonfüzfő 8175, Irinyi utca 8. 8/5

Firmenregisternummer: 19-09-508818

E-Mail: molnartsa@freemail.hu

Telefon: 30/431-6373

#### **FourMed Egészségügyi Szolgáltató Kft.**

Firmensitz: Veszprém 8200, Kabay János utca 2.

Firmenregisternummer: 19-09-502293

E-Mail: fourmed@gmail.com

Telefon: 0688-421-251

#### **CODEBASE Szoftverfejlesztő, Kereskedelmi és Szolgáltató Kft.**

Firmensitz: 103 7 Budapest, Bokor utca 15. 1. Et. 27.

Firmenregisternummer: 01-09-725607

Steuernummer: 13246422-2-41

#### **Macrotel Kft.**

Firmensitz: Veszprém 8200, Gerenda út 4.

Firmenregisternummer: 19-09-506709

E-Mail: pichnerp@marcotel.hu

Telefon: 003630/283-8063

#### **Signator Audit Könyvvizsgáló Kft.**

Firmensitz: Veszprém 8200, Radnóti tér 2

Firmenregisternummer: 19-09-500315

E-Mail: signator@signator.hu

Telefon: 0630/901-2777

**Csapó, Kiss és Mohos Ügyvédi Iroda (Anwaltskanzlei)**

Firmensitz: Veszprém 8200, Ádám Iván u 10.

Telefon: 003630/946-3452

**Veszprém-Balaton Régió Kultúrájáért Közalapítvány (Öffentliche Stiftung für die Kultur der Region Veszprém-Balaton)**

Firmensitz: Veszprém 8200, Óváros tér 9.

Registernummer: 19-01-0000227

Die vorliegenden Bestimmungen müssen im Einklang mit den Vorschriften der üblichen Regelungen der Organisation gedeutet werden. Wenn bezüglich des Schutzes personenbezogener Daten zwischen den vorliegenden Bestimmungen und den Vorschriften jeglicher anderer, vor dem Inkrafttreten der vorliegenden Regelung in Kraft getretener Regelung ein Widerspruch bestehen sollte, so sind die Bestimmungen der vorliegenden Regelung maßgebend.

## **In der vorliegenden Regelung verwendete Abkürzungen:**

**InfoG** Gesetz Nr. CXII vom Jahre 2011 über das Informationsselbstbestimmungsrecht und der Informationsfreiheit

**DSGVO** Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)

**ArbGB** Gesetz Nr. 1 vom Jahre 2012 das Gesetzbuch der Arbeit

**ArbSchG** Gesetz Nr. XCIII vom Jahre 1993 über den Arbeitsschutz

**BGB** Gesetz Nr. V vom Jahre 2013 über das Bürgerliche Gesetzbuch

**PVG** Gesetz Nr. CXXXIII vom Jahre 2005 über die Regeln der Tätigkeiten für Personen- und Vermögensschutz, und der Privatdetektive

**NAIH** oder Behörde, Nationale Behörde für Datenschutz und Informationsfreiheit

## **2. ALLGEMEINE BESTIMMUNGEN**

### **2.1. Zweck und Gültigkeit der Regelung**

Zweck der vorliegenden Vorschriften ist die Regelung der Führung der im Laufe der Tätigkeit der Organisation geführter Register im Einklang mit den Bestimmungen der DSGVO, die Sicherstellung der gesetzlichen Ordnung der Datenverarbeitung und der damit verbundenen Datenschutzregelung, die Geltendmachung des mit dem Schutz personenbezogener Daten verbundenen Informationsselbstbestimmungsrechtes und der Datensicherheit, die Vorbeugung von unbefugten Zugriffen, der Veränderung der Daten, der unbefugten Veröffentlichung und jeglicher unbefugter Nutzung.

Der persönliche Wirkungsbereich der Regelung erstreckt sich auf die Funktionsträger, Praktikanten, Vertragspartner, Kunden der Organisation und ihrer Partner.

Bei der Anwendung der Regelung müssen auch Einzelunternehmer, Einzelunternehmen, Primärerzeugerkunden, Käufer und Lieferanten als natürliche Personen behandelt werden. Die Gültigkeit der Regelung erstreckt sich gleichzeitig aber nicht auf so eine Verwaltung personenbezogener Daten, die sich auf juristische Personen, bzw. die sich besonders auf solche Unternehmen erstreckt, die als juristische Personen gegründet worden sind, darunter verstanden auch den Namen und die Form der juristischen Person, wie auch Angaben bezüglich der Kontaktdaten der juristischen Person, aber die für die Kontaktpflege der Kontaktperson der juristischen Person notwendige personenbezogene Daten fallen unter die Gültigkeit der Regelung.

Der sachliche Anwendungsbereich der Regelung erstreckt sich auf folgendes:

- alle bei der Organisation entstandene Daten, unabhängig von ihrer Erscheinungsform;
- die in dem IT-System verwalteten oder verarbeiteten Daten;
- die als Ergebnis der Datenverarbeitung entstandene Daten;
- alle bei der Organisation verwendete Hardware- und Software Mittel, als Datenschutzmittel;
- mit der Tätigkeit der Organisation verbundene, im Laufe ihrer Tätigkeit entstehende Daten von öffentlichem Interesse oder aus öffentlichem Interesse öffentliche Daten.

### **2.2. Grundbegriffe des Datenschutzes**

Das Begriffssystem der vorliegenden Regelung ist übereinstimmend mit den in Artikel 4 der DSGVO festgelegten Begriffserklärungen. Dementsprechend lauten die Hauptbegriffe:

- „personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als

identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann;

- „Verarbeitung“ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;
- „Einschränkung der Verarbeitung“ die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken;
- „Profiling“ jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen;
- „Pseudonymisierung“ die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden;
- „Dateisystem“ jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird;
- „Verantwortlicher“ die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden;
- „Auftragsverarbeiter“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet;
- „Empfänger“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht. Behörden, die im Rahmen eines bestimmten Untersuchungsauftrags nach dem Unionsrecht oder dem Recht der Mitgliedstaaten möglicherweise personenbezogene Daten erhalten, gelten jedoch nicht als Empfänger; die Verarbeitung dieser Daten durch die genannten Behörden erfolgt im Einklang mit den geltenden Datenschutzvorschriften gemäß den Zwecken der Verarbeitung;
- „Dritter“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten;
- „Einwilligung“ der betroffenen Person jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist;
- „Verletzung des Schutzes personenbezogener Daten“ eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder

zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden;

- „Gast“: eine natürliche Person, betroffene Person, die von, sich auf dem Gebiet der Organisation befindenden, bzw. mit ihr in einem Vertragsverhältnis stehenden Dienstleistern Dienstleistungen in Anspruch nimmt, bzw. eine Absichtserklärung über die Inanspruchnahme abgegeben hat
- „Datenbesitzer“: der Leiter jener Organisationseinheit, wohin nach den gesetzlichen Vorschriften oder den öffentlich-rechtlichen organisationsregelnden Mitteln die Entstehung der Daten zuordnet wird, bzw. wo die Daten entstehen.

### **3. METHODOLOGISCHE REGELN DER VERARBEITUNG PERSONENBEZOGENER DATEN**

#### **3.1. Grundsätze bezüglich der Verarbeitung personenbezogener Daten**

##### **Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz**

Die Verarbeitung personenbezogener Daten darf nur anhand einer Rechtsgrundlage (Zustimmung oder eine andere gesetzliche Rechtsgrundlage) erfolgen. Die personenbezogenen Daten müssen nach Treu und Glauben, auf eine für die Betroffenen transparente Weise verarbeitet werden. Die sich auf die Datenverarbeitung beziehende Informationen müssen in einer genauen, transparenten, verständlichen und leicht zugänglichen Form, mit einfachem und verständlichem Sprachgebrauch angegeben werden.

##### **Zweckbindung**

Personenbezogene Daten dürfen nur für festgelegte, eindeutige und legitime Zwecke erhoben werden. Die Weiterverarbeitung der Daten darf auch nur auf einer damit zu vereinbarenden Weise erfolgen. Eine mit der Zweckbindung direkt zusammenhängende Abwägung zwischen den Interessen des Verantwortlichen und der Betroffenen erschafft in vielen Fällen die Rechtsgrundlage der Datenverarbeitung. Daher muss der Zweck der Datenverarbeitung in jedem Fall festgelegt werden.

##### **Datenminimierung**

Im Sinne des Grundsatzes der Datenminimierung ist die Erhebung und Datenverarbeitung auf jene Daten zu begrenzen, welche für ein Erreichen des erwünschten Zwecks tatsächlich notwendig sind.

##### **Richtigkeit**

Im Laufe der Datenverarbeitung muss auf nachweisbare Weise sichergestellt werden, dass die Daten sachlich richtig, vollständig und auf dem neuesten Stand sind; wie auch ein Löschen oder eine Berichtigung unrichtiger Daten sichergestellt werden muss. Zum Zwecke der Erfüllung dieses Grundsatzes durch unsere Gesellschaft, oder in der Organisation unserer Gesellschaft, ist unsere Gesellschaft verpflichtet routinemäßige Verfahren zur Aktualisierung der verarbeiteten personenbezogenen Daten einzuführen.

##### **Speicherbegrenzung**

Das Speichern personenbezogener Daten, die die Identifizierung der betroffenen Personen ermöglicht, ist nur so lange möglich, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. Weiterhin müssen auch die gesetzlich vorgeschriebenen Fristen eingehalten werden.

##### **Integrität, Vertraulichkeit**

Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen. Dazu müssen in erster Linie aus IT- und organisatorischer Sicht (z.B. Verfahrensordnung für berechtigte Zugriffe und Berechtigungen, Codierung) geeigneten Maßnahmen ergriffen werden, unter besonderer Berücksichtigung der in den Artikel 32 (Sicherheit der Datenverarbeitung) und Artikel 35 (Folgenabschätzung der Datenverarbeitung) der DSGVO erfasster Bestimmungen.

##### **Rechenschaftspflicht**



Im Sinne von Absatz 2, Artikel 5 der DSGVO muss unsere Gesellschaft anhand des Grundsatzes der Rechenschaftspflicht eine Entsprechung der vorausgehend vorgestellter Grundsätze mit Dokumenten unterstützt nachweisen können.

### **3.2. Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten**

Gemäß Artikel 6 DSGVO die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

- Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;
- die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;
- die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;
- die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;
- die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;
- die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Die Organisation führt ihre Tätigkeit während der Datenverarbeitung anhand folgender Gesetzesvorschriften durch:

- Grundgesetz von Ungarn
- Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG
- Gesetz Nr. CXII vom Jahre 2011 über das Informationsselbstbestimmungsrecht und der Informationsfreiheit (InfoG)
- Gesetz Nr. LXVI vom Jahre 1992 über die Registrierung personenbezogener Daten und Adressen der Bürger,
- Gesetz Nr. CLV vom Jahre 2009 über den Schutz qualifizierter Daten,
- Gesetz Nr. CXXXIII vom Jahre 2005 über die Regeln der Tätigkeiten für Personen- und Vermögensschutz, und der Privatdetektive (PVG)
- Gesetz Nr. VI vom Jahre 1998 über die Verkündung des im Strasbourg am 28. Januar 1981 datierten Abkommens über den Schutz des Individuums bei der maschinellen Verarbeitung personenbezogener Daten
- Gesetz Nr. CL vom Jahre 2016 über die allgemeine Verwaltungsordnung
- Gesetz Nr. V vom Jahre 2013 über das Bürgerliche Gesetzbuch (BGB)
- Gesetz Nr. c vom Jahre 2000 über das Rechnungswesen
- Gesetz Nr. CLV vom Jahre 1997 über den Verbraucherschutz
- Gesetz Nr. CXVII vom Jahre 1995 über die Einkommenssteuer
- Gesetz Nr. XCIII vom Jahre 1993 über den Arbeitsschutz (ArbSchG)
- Gesetz Nr. 1 vom Jahre 2012 das Gesetzbuch der Arbeit (ArbGB)
- Gesetz Nr. CVIII vom Jahre 2001 über die einzelnen Fragen der elektronischen Handelsdienstleistungen, und den mit der Informationsgesellschaft zusammenhängender Dienstleistungen
- Gesetz Nr. CLIV vom Jahre 1997 über das Gesundheitswesen (GwG)
- Gesetz Nr. XLVII vom Jahre 1997 über die Verarbeitung und dem Schutz von gesundheitlichen und damit verbundenen personenbezogenen Daten (GDVG)

#### 4. BEI DER ORGANISATION STATTFINDENDE DATENVERARBEITUNGEN

##### 4.1. Datenverarbeitung bezüglich der Gründung, Aufrechterhaltung und dem Beenden eines Arbeitsverhältnisses

Prozess einer Arbeitsbewerbung bei der Organisation:

Für die Auswahl eines geeigneten Arbeitnehmers sind der Geschäftsführer, der Leiter der zuständigen Organisationseinheit, bzw. die HR-Abteilung verantwortlich, die in Zusammenarbeit mit dem Datenschutzbeauftragten verpflichtet sind bei dem Versehen der mit der vorliegenden Datenverarbeitung verbundenen Aufgaben die Rechte der Betroffenen sicherzustellen.

Bei der Auswahl von Arbeitskräften eröffnen sich personenbezogene Daten vor der Organisation auf folgende Weise:

Die Werbung für Arbeitskräfte erfolgt über in der Presse und im Internet veröffentlichten Anzeigen, weiterhin kann die Organisation auch unter ihren eigenen Mitarbeitern und auf Empfehlung Arbeitnehmer für leere Arbeitsstellen suchen, bzw. kann die Auswahl auch unter Bewerbern ohne eine Anfrage erfolgen. Die Organisation unterscheidet die für eine Stellenbewerbung eingereichte, personenbezogene Daten beinhaltende Lebensläufe (im Weiterem: CV oder Lebenslauf) nicht nach der Art ihrer Einreichung: die auf Papier und auf elektronische Weise eingereichten Lebensläufe werden gleichbehandelt. Bei einer Bewerbung für ein konkretes Stellenangebot verwaltet die Organisation die Lebensläufe ab ihrem Zusenden an die Organisation, bzw. ab dem Abschluss der Bewerbung höchstens 6 Monate lang, in welchem Zeitraum der Bewerber jederzeit das Beenden der Datenverarbeitung beantragen kann. Wenn die Organisation die Daten des Bewerbers für einen längeren Zeitraum bearbeiten möchte, holt sie dazu von dem Bewerber eine gesonderte Ermächtigung ein.

Die bei der [hr@veszprembalaton2023.hu](mailto:hr@veszprembalaton2023.hu) E-Mail-Adresse in jeglicher Form und zu jeglichem Zweck eingereichte Bewerbungen werden von dem Postsystem der Organisation gespeichert, bzw. werden diese in die innerhalb der auf dem Netzwerk gespeicherten Personalabteilungsmappe definierte Mappe gespeichert. Die HR-Abteilung versendet in jedem Fall ein Antwortschreiben, in dem die Bewerber über die Aufbewahrung oder dem Löschen des Lebenslaufes, bzw. über weitere Entscheidungen informiert werden.

Zweck der Verarbeitung	Kreis der verarbeiteten Daten	Rechtsgrundlagen für die Verarbeitung	Speicherfrist	Art der Datenspeicherung
Zum Besetzen leerer Arbeitsstellen. Zum Zwecke einer späteren Gründung eines Arbeitsverhältnisses, zur Auswahl geeigneter zukünftiger Arbeitnehmer	Name, Geburtsdatum, Name der Mutter, Wohnadresse, Ausbildungsangaben, vom Betroffenen angegebene weitere Angaben, Personenidentifikation der empfehlenden Person, Fakten einer erfolgreichen Hintergrundüberprüfung	Freiwillige Zustimmung der Betroffenen [Punkt a) Artikel 6 der DSGVO, welche Zustimmung die Betroffenen durch das Zusenden der Lebensläufe und der damit verbundenen Dokumente erteilen.]	Bis zum Löschantrag der Betroffenen, höchstens 1 Jahr lang ab ihrer Zustellung	Auf Papier, elektronisch

Die Organisation überprüft die Arbeitsplatzzeignung ihrer Arbeitnehmer entsprechend der gesetzlichen Vorschriften regelmäßig. Die Organisation steht entsprechend ihrer gesetzlichen Verpflichtungen in einem Vertragsverhältnis mit einem arbeitsmedizinischen Facharzt. Die Organisation erfährt die Gesundheitsdaten bezüglich der Arbeitsplatzzeignung nicht, und sie verarbeitet die Daten keiner betroffenen Person in einer den Zweck überschreitenden Weise. Die Organisation verarbeitet nur die Tatsache einer Arbeitseignung nachweisende Daten.

Die Organisation erstellt - im Einklang mit dem Standpunkt der Nationalen Behörde für Datenschutz und Informationsfreiheit – zur Identifizierung natürlicher Personen keine Kopien von Nachweisdokumenten der Personalien. Zur Einhaltung des Prinzips der Datenerfassung und der Datenqualität kann aber die Organisation die Identifikationsausweise neu eintretender oder ihre Daten verändernder Mitarbeiter zur Einsicht einverlangen.

#### 4.2. Lohn- und Arbeitsverzeichnis

Die Organisation führt über ihre Mitarbeiter ein Personal-, bzw. Lohn- und Arbeitsverzeichnis. Die Organisation speichert die Daten eingestellter Arbeitnehmer sowohl auf Papier, als auch elektronisch. Jene personenbezogenen Daten der Arbeitnehmer werden aufgenommen, die zur Gründung eines Arbeitsverhältnisses notwendig sind.

Die Daten des Personenregisters dürfen zur Feststellung der mit dem Arbeitsverhältnis des Arbeitnehmers zusammenhängender Tatsachen, und für statistische Datendienstleistungen verwendet werden. Bezüglich der Verarbeitung der Arbeitnehmerdaten ist eine Aufklärung für Arbeitnehmer erstellt worden, deren Ziel eine vorangehende Aufklärung der Arbeitnehmer über die Datenverarbeitung ist.

Die bezüglich eines Arbeitsverhältnisses erhaltene Daten einer Drittperson (zum Beispiel bezüglich Zusatzurlaub, familiäre Steuervergünstigung, oder bei der Abgabe der Kontaktpersonen bei einem Unfall) dürfen nur den notwendigen Datenumfang nicht überschreitend aufgenommen und verarbeitet werden.

Zweck der Verarbeitung	Kreis der verarbeiteten Daten	Rechtsgrundlage für die Verarbeitung	Speicherfrist	Art der Datenspeicherung
Gründung, Aufrechterhaltung und das Beenden eines Arbeitsverhältnisses, Anerkennung der damit verbundenen Berechtigungen und Bezeugen der Verpflichtungen.	Siehe unter der Tabelle	Gesetzliche Bevollmächtigung [Punkt c) Absatz (1) der DSGVO] ((1) und (3) §10 des ArbGB], und die zutreffenden Bestimmungen der Steuer- und Sozialversicherungsgesetze	5 Jahre lang ab dem Beenden der Arbeitsverhältnisses oder dem Erlangen des Rentenalters.	Auf Papier und elektronisch

#### Kreis der verwalteten Daten

Name, Geburtsname, Geburtsort und Datum, Staatsbürgerschaft, Geburtsname der Mutter. Wohnadresse, Aufenthaltsort (wenn von der Wohnadresse abweichend), private Rentenversicherung [Fakt der Mitgliedschaft, Eintrittsdatum (Tag, Monat, Jahr), Name und Code der Bank, Steuerkennzeichen], Sozialversicherungszeichen (Sozialversicherungsnummer), Rentner Stammzahl (bei Rentnern als Arbeitnehmer), Kopie des Arbeitsbuches (wenn es ein solches gibt), Girokontonummer, Anfangstag des Arbeitsverhältnisses, Typ des Versicherungsverhältnisses, Anzahl

der wöchentlichen Arbeitsstunden, Telefonnummer, Familienstand, Kopie Exemplar der Ausbildungsdokumente, arbeitsmedizinische Eignungsbescheinigung, Arbeitskreis, Tatsache der medizinischen Eignung, Führungszeugnis [Datum der Erstellung, Urkundennummer, ID des Antrages], nach der Abrechnung, Fakt der Durchführung der ärztlichen Eignungsuntersuchung für den Arbeitskreis, Gutachterbeschluss zur Begründung einer verminderten Arbeitsfähigkeit bei Mitarbeitern mit verminderter Arbeitsfähigkeit, bei einer Arbeitsausführung außerhalb des Hauptarbeitsplatzes [Art des Rechtsverhältnisses Name und Sitz des Arbeitgebers, durchschnittlich monatlich erfüllte Arbeitszeit auf dem Arbeitsplatz außerhalb des Hauptarbeitsplatzes, durchzuführende Tätigkeit], Bescheinigungen bezüglich des vorherigen Arbeitsverhältnisses [Nachweise über Versichertenrechtsstand und der Sozialversicherungsversorgung, Arbeitgeberbescheinigung über das Beenden des Rechtsverhältnisses, Steuerformular des Vorjahres], bezüglich der Inanspruchnahme von anhand § 120 des ArbGB zustehendem Zusatzurlaub [Kopie des Dokumentes zum Nachweis der Feststellung einer veränderten Arbeitsfähigkeit durch das Gutachterorgan für Rehabilitation, Kopie der Urkunde zum Nachweis der Berechtigung zur Behindertenunterstützung, Kopie der Urkunde zum Nachweis der Berechtigung zur Blindenrente], Inanspruchnahme von Zusatzurlaub, familiäre Steuervergünstigung, Antrag von als steuerfreie Zuwendungen in Naturalien geltendem vergünstigtem Reiseausweis, oder zum Zwecke der steuerfreien Schulanfangsunterstützung eines a) das 16. Lebensjahr nicht vollendeten Angehörigen, b) eines das 16. Lebensjahr vollendeten Angehörigen, Lebensgefährten des Arbeitnehmers [Name, Geburtsname, Geburtsort und Datum, Wohnadresse, Name der Mutter, Sozialversicherungszeichen (Sozialversicherungsnummer), Steuerkennzeichen, Tatsache des Vorhandenseins eines gültigen Studentenausweises].

#### 4.3. Arbeitsschutz, Brandschutz, Unfallschutz

Die Erstellung, Instandhaltung der Arbeitsschutzregelung der Organisation, und die Durchführung bestimmter mit dem Arbeitsschutz verbundener Schulungen, bzw. mit Kontrollen verbundene fachliche Tätigkeit wird von einem externen Experten anhand eines Auftragsvertrages durchgeführt. Die Organisation übergibt dem beauftragten Unternehmen keine personenbezogenen Daten der Arbeitnehmer, aber im Laufe der mit dem Arbeitsschutz verbundener Verfahren, bzw. der regelmäßigen Schulungen, bei eventuellen Arbeitsunfällen, bzw. der Kontrollen nimmt, bzw. verarbeitet das beauftragte Unternehmen, im Interesse des Auftraggebers verfahrens, von den Betroffenen personenbezogene Daten auf.

Zweck der Verarbeitung	Kreis der verarbeiteten Daten	Rechtsgrundlage für die Verarbeitung	Speicherfrist	Art der Datenspeicherung
Untersuchung von Arbeitsunfällen, Berufserkrankungen und erhöhter Expositionen	Name der Mutter, Sozialversicherungszeichen (Sozialversicherungsnummer), Geburtsort und Datum, Geschlecht, Staatsbürgerschaft, Wohnort (Wohnadresse)	Gesetzliche Bevollmächtigung [Punkt c) Absatz (1) der DSGVO] (Absatz (3) des ArbSchG)	Zur Geltendmachung der anhand des Untersuchungsergebnisses begründeter Forderungen zur Verfügung stehende Frist	Elektronisch und auf Papier

#### 4.4. Datenverarbeitung bezüglich der Firmenhandys der Arbeitnehmer:

Die Handynutzungsregelung der Organisation beinhaltet die Bestimmungen bezüglich der Nutzung von Firmenhandys.

#### 4.5. Praktikanten

Die Organisation beschäftigt Praktikanten anhand Gesetz Nr. 1 vom Jahre 2012 über das Gesetzbuch der Arbeit, §44 des Nr. CCIV Gesetzes vom Jahre 2011 über die nationale Hochschulausbildung, und § 17 und § 18 der Nr. 230/2012 Regierungsverordnung (vom 28.08.) über die einzelnen Fragen der Hochschulen Fachausbildung und der mit der Hochschulausbildung verbundenen fachlichen Praxis, weiterhin anhand der mit den einzelnen Institutionen abgeschlossenen Kooperationsvereinbarungen. Während der Arbeitsdurchführung gelten für die Praktikanten die gleichen Regeln, wie für die Arbeitnehmer der Organisation.

Mit den Praktikanten werden gesonderte Praktikantenverträge unterzeichnet. Anhand der Verträge und der gesetzlichen Verpflichtungen ist die Datenverarbeitung von Praktikanten Folgende:

Zweck der Verarbeitung	Kreis der verarbeiteten Daten	Rechtsgrundlage für die Verarbeitung	Speicherfrist	Art der Datenspeicherung
Gründung, Aufrechterhaltung und das Beenden eines Praktikantenverhältnisses	Name, Geburtsname, Geburtsname der Mutter, Geburtsort und Datum, Wohnadresse, Studenten-ID, Telefonnummer, E-Mail- Adresse, Steuerkennzeichen , Bankkontonummer	[Punkt c), Abs. (1), Art. 6 der DSGVO] ((1) und (3) § 10 des ArbGB), und die zutreffenden Bestimmungen der Steuer- und Sozialversicherungs-gesetze, Punkt b) § 18/B der Reg. Verord. Nr. 230/2012	2 Jahre ab dem Beenden des Praktikantenverhältnisses	Auf Papier und elektronisch

#### 4.6. Datenverarbeitung bezüglich des Betriebens von Seiten der sozialen Medien

Die Organisation betreibt eine eigene Webseite unter [www.veszprembalaton2023.hu](http://www.veszprembalaton2023.hu). Die Organisation veröffentlicht auf der Webseite die wichtigsten Informationen bezüglich ihrer Tätigkeit, der durch sie geworbener Ereignisse, Programme. Zur Verbesserung des Besuchererlebnisses und zum Zwecke des Sammelns statistischer Daten verwendet die Organisation Cookies.

Die Organisation überprüft halbjährlich mit Hilfe automatisierter Abfragen die Cookie Einstellungen der Webseite, und hält in ihren Datenschutzgrundsätzen auf der Webseite die verwendeten Cookies ständig auf dem aktuellen Stand.

Zur Vorstellung der Tätigkeit, des Aufbaus, der Stellenmöglichkeiten, der mit der Firma verbundener Neuigkeiten, und der durch die Organisation, oder unter Mitwirkung der Organisation organisierter Ereignisse betreibt die Organisation mit Hilfe folgender Auftragsverarbeiter Facebook, Instagram, LinkedIn, YouTube Seiten.

Durch das Klicken auf den „Teilen“-Link der in den sozialen Medien durch die Organisation betriebener Seiten, geben die Betroffenen ihre Zustimmung zur Veröffentlichung der Nachrichten und Angebote der Organisation auf ihrer Pinnwand. Die Organisation veröffentlicht auf diesen Seiten über die verschiedenen Ereignisse usw. auch Bilder/Filme. Wenn es sich nicht um Massenaufnahmen handelt, holt unsere Gesellschaft vor der Veröffentlichung der Aufnahmen immer die schriftliche Zustimmung der Betroffenen ein.

Über die Datenverarbeitung auf den Seiten der sozialen Medien können Sie sich auf den Webseiten dieser befindlichen Datenschutz Grundsätze und Regelungen informieren.

Zweck der Verarbeitung	Kreis der verarbeiteten Daten	Rechtsgrundlage für die Verarbeitung	Speicherfrist	Art der Datenspeicherung
Vorstellung, Förderung der Tätigkeit, des Aufbaus, der Stellenmöglichkeiten, der Neuigkeiten der Organisation	IP-Adresse, statistische Cookies, auf Seiten der sozialen Medien Daten anhand der Datenschutzregelungen der sozialen Medien durch die Seiten der sozialen Medien	Freiwillige Zustimmung der Betroffenen [Punkt a) Absatz (1) Artikel 6 der]	Datum der Aufrechterhaltung der Webseite, 10 Jahre ab der Annahme der Abschlussabrechnung des VEB2023 Projektes.	Elektronisch

#### 4.7. Datenverarbeitung bezüglich Marketing, Newsletter:

Ziel der Marketingtätigkeit ist die Förderung der Programmreihe „**Kulturhauptstadt Europas Veszprém-Balaton 2023**“, ein Kennenlernen der Tätigkeit der Organisation in einem weitmöglichsten Kreis.

Für die Kontaktpflege mit unseren Gästen und der Förderung unserer Dienstleistungen betreibt die Organisation einen regelmäßigen oder fallweisen Newsletter um Kontakt mit den Partnern der Organisation zu halten, Informationen über die wichtigsten Ereignisse, Veranstaltungen, Daten zu geben.

Zweck der Verarbeitung	Kreis der verarbeiteten Daten	Rechtsgrundlage für die Verarbeitung	Speicherfrist	Art der Datenspeicherung
Kontakthaltung mit den potentiellen Partnern, Versenden von Newsletter über Veranstaltungen und verbundene Informationen	Name, E-Mail-Adresse	Zustimmung der Betroffenen, und das berechnete Interesse des Verantwortlichen die mit dem Partner ausgebildete Geschäftsbeziehungen aufrecht zu erhalten, zu entwickeln [Punkt a) bzw. f) Abs. (1) Artikel 6 der DSGVO]	Bis zur Abmeldung des Newsletters – über eine an den Verantwortlichen adressierte E-Mail, oder das Klicken auf das Zeichen „Abmeldung“ im Newsletter	Elektronisch

#### 4.8. Datenverarbeitung bezüglich Bewerbungen

Die Organisation veröffentlicht auf ihrer Webseite Bewerbungsausschreibungen in verschiedenen Bereichen, wozu wir auch personenbezogene Daten verarbeiten. Solche Themenbereiche sind Kooperation, Projektverwirklichung.

Zweck der Verarbeitung	Kreis der verarbeiteten Daten	Rechtsgrundlage für die Verarbeitung	Speicherfrist	Art der Datenspeicherung
Kontaktpflege mit den Bewerbern, Koordinierung,	Kontaktdaten der Bewerber, bzw. der	Zustimmung der Betroffenen, welche gleichzeitig	10 Jahre ab der Annahme der Abschlussabrechnung	Elektronisch und auf Papier

Abrechnung der Durchführung bei den Gewinnerbewerbungen	Kontaktpersonen der Bewerber (Name, E-Mail-Adresse am Arbeitsplatz, Telefonnummer)	mit dem Einreichen der Bewerbung, auf dem Bewerbungsformular erteilt wird.  Das berechnete Interesse des Verantwortlichen die mit dem Partner ausgebildete Geschäftsbeziehungen aufrecht zu erhalten, zu entwickeln [Punkt a) bzw. f) Abs. (1) Artikel 6 der DSGVO]	ung des VEB2023 Projektes.	
---	--	---	----------------------------	--

## 5. DATENSCHUTZSYSTEM DER ORGANISATION

### 5.1. Datenschutzorganisation innerhalb der Organisation

Die Direktion der Organisation bestimmt unter Berücksichtigung der Merkmale der Organisation die Organisation für Datenschutz, die Aufgaben- und Wirkungskreise bezüglich des Datenschutzes und der damit verbundenen Tätigkeiten, und legt die Aufsicht der Datenverarbeitung versehenden Person fest.

Die Mitarbeiter der Organisation sorgen während ihrer Arbeit dafür, dass unbefugte Personen keine Einsicht in die personenbezogenen Daten erlangen, wie auch dafür, dass der Aufbewahrungsort, die Unterbringung der personenbezogenen Daten so gestaltet ist, dass unbefugte Personen auf diese keinen Zugriff haben, sie diese nicht kennenlernen, verändern, vernichten können.

(1) § 11/A des ArbGB kann im Kreis des mit dem Arbeitsverhältnis zusammenhängenden Verhaltens des Arbeitnehmers überprüft werden. Im Rahmen dessen kann der Arbeitgeber auch technische Mittel verwenden, worüber er den Arbeitnehmer im Vorfeld schriftlich informiert.

(2) Der Arbeitnehmer darf die vom Arbeitgeber zur Arbeitsdruchführung zur Verfügung gestellte Informationstechnologische oder Computertechnologische Mittel, Systeme (im Weiterem: Computertechnologische Mittel) – Mangels einer abweichenden Vereinbarung – ausschließlich zum Zwecke der Erfüllung des Arbeitsverhältnisses nutzen.

(3) Während der Kontrolle ist der Arbeitgeber berechtigt Einsicht in die sich auf den zum Zwecke der Erfüllung des Arbeitsverhältnisses genutzten Computertechnologische Mittel befindlichen Daten zu bekommen.

(4) Aus Sicht der Kontrollberechtigung anhand des Absatzes (3) gelten als mit dem Arbeitsverhältnis zusammenhängende Daten die für die Kontrolle der Einhaltung der in Absatz (2) festgelegten Begrenzung notwendige Daten.

Die Direktion versieht die Aufsicht des Datenschutzsystems der Organisation, auf dem Wege eines durch sie beauftragten Datenschutzbeauftragten.

Die Organisation stellt den Datenschutzbeauftragten die für seine Aufgabenerfüllung notwendige Ressourcen zur Verfügung, weiterhin stellt sie ihm auch sicher, dass er während dem Versehen seiner Aufgaben von keinen Weisungen annimmt, er im Zusammenhang mit der Erfüllung dieser Aufgaben nicht gekündigt oder durch Sanktionen bestraft werden kann. Der Datenschutzbeauftragte schuldet organisatorisch direkt dem Geschäftsführer der Organisation Rechenschaft.

#### Aufgaben der Direktion bezüglich des Datenschutzes:

- Verantwortlichkeit für die Sicherstellung der zum Schutz der durch die Organisation verarbeiteter personenbezogener Daten notwendiger personeller, sachlicher und technischer Bedingungen;
- Verantwortlichkeit für das Beenden der bei den Kontrollen der Datenverarbeitung eventuell vorgefundener Mängel oder rechtsverletzender Umstände
- Verantwortlichkeit für das Einleiten, bzw. das Durchführen eines Verfahrens zur Feststellung der persönlichen Verantwortung;
- Aufsicht der Tätigkeit des Datenschutzbeauftragten;
- Anordnung von Untersuchungen;
- Ausgabe der internen Regelungen der Organisation bezüglich des Datenschutzes.

#### Aufgaben des Datenschutzbeauftragten bezüglich des Datenschutzes:

- Teilnahme, bzw. Hilfe bei der Entscheidungsfindung bezüglich Fragen des Datenschutzes, Hilfeleistung bei der Sicherstellung der Rechte der Betroffenen;
- Erstellen eines Berichtes für die Direktion über die Durchführung der Datenschutzaufgaben der Organisation bis zum 15. Januar jeden Jahres;
- Berechtigung zur Kontrolle der Einhaltung der vorliegenden Regelung bei den einzelnen Organisationseinheiten;
- Führen des Verzeichnisses für interne Datenverarbeitung und Datenweiterleitung;
- Teilnahme an der durch die Nationale Behörde für Datenschutz und Informationsfreiheit veranstalteten Konferenz für Datenschutzbeauftragter;
- Beobachtung der Gesetzesveränderungen bezüglich des Datenschutzes und der Informationsfreiheit, anhand dessen in begründeten Fällen die Einleitung der Modifizierung der vorliegenden Regelung;
- Teilnahme an der Beantwortung der durch die Nationale Behörde für Datenschutz und Informationsfreiheit an die Organisation gestellter Fragen, und an einer durch die Nationale Behörde für Datenschutz und Informationsfreiheit eingeleiteten Untersuchung, bzw. an einem Verfahren einer Behörde für Datenschutz;
- Formulieren einer Anfrage an die Nationale Behörde für Datenschutz und Informationsfreiheit zum Zwecke einer allgemeinen Stellungnahme, wenn eine aufgetauchte Frage anhand der Rechtsdeutung nicht eindeutig beantwortet werden kann;
- Kontrolle der Eignung der Rechtsvorschriften für Datenschutz, und der internen Regelungen der Organisation, darunter verstanden auch das Festlegen der Aufgabenbereiche, die Bewusstseinsförderung und Schulung der an den Operationen der Datenverarbeitung betroffener Personen, wie auch das Festlegen verbundener Audits;
- Schulungen über Datenschutzkenntnisse;
- Teilnahme an der Bearbeitung der bei der Organisation bezüglich des Datenschutzes eingereichter Anfragen, Fragen, Beschwerden, Durchführen der weiteren mit dem Datenschutz verbundener, gesetzlich mit der Funktion verbundener Aufgaben

#### Aufgaben des IT-Leiters bezüglich des Datenschutzes:

- Teilnahme, Hilfestellung bzw. Unterbreiten von Vorschlägen an den internen Datenschutzbeauftragten bei der Vorbereitung von Entscheidungen, die mit IT-Datenverarbeitung zusammenhängen;
- Kontrolle der Einhaltung der sich auf IT-Datenverarbeitung beziehender gesetzlicher Vorschriften, bzw. der zutreffenden internen Regelungen bezüglich der Anforderungen der Datensicherheit;
- Teilnahme an der Klärung und Ausarbeitung der die Informatik betreffender Fragen des internen Datenschutzes und der Regelung für Datenverarbeitung;
- Sicherstellung des IT-Hintergrundes der Führung des internen Datenverarbeitungsverzeichnisses;
- Erfüllung der gegenüber dem Datenschutzbeauftragten bestehender Verpflichtungen;



- Unterbreiten von Vorschlägen an den Datenschutzbeauftragten bezüglich Maßnahmen über den Datenschutz;
- Aktualisieren/Aktualisieren lassen der Informatik Sicherheitsregelung;
- Erstellen eines schriftlichen Berichtes an den Datenschutzbeauftragten über die IT-Realisierung des Datenschutzes nach Bedarf, aber mindestens einmal jährlich (bis zum 31. Oktober jeden Jahres).

#### **Aufgaben der Leiter der einzelnen Organisationseinheiten bezüglich des Datenschutzes:**

- Verantwortung für die Entsprechung der Datenverarbeitungen ihrer Organisationseinheiten an den Gesetzesvorschriften und der vorliegenden Regelung, oder der verbundenen Regelungen;
- Verantwortung für die vollständige Erfüllung der Datenschutzvorschriften aus Teil 5.2 der vorliegenden Regelung bei den Datenverarbeitungen ihrer Organisationseinheiten;
- Kontrolle der Einhaltung der mit Datenschutz verbundener Vorschriften, so besonders der Bestimmungen der vorliegenden Regelung;
- Verlangen bei dem Datenschutzbeauftragten um Hilfe, wenn Fragen bezüglich der Verarbeitung personenbezogener Daten, Geschäftsgeheimnissen, Daten von öffentlichem Interesse auftauchen;
- Zusammenarbeit mit dem Datenschutzbeauftragten zum Zwecke der Erfüllung der mit dem Datenschutz verbundener Regeln;
- Sicherstellen dessen, dass ihre Angestellten an den durch den Datenschutzbeauftragten organisierten, bzw. gehaltenen Schulungen zum Datenschutz teilnehmen können.

#### **Aufgaben die personenbezogenen Daten verarbeitender Arbeitnehmer bezüglich des Datenschutzes:**

- Verarbeitung und Bewahrung der im Laufe der Aufgabenerfüllung in den Besitz gelangter Daten;
- Achten auf eine sichere Handhabung und Aufbewahrung der personenbezogenen Daten beinhaltender Verzeichnisse;
- Sorgen dafür, dass keine unbefugten Personen Zugriff zu den durch sie behandelten Daten haben;
- Einhaltung der sich auf den Datenschutz beziehender Gesetzesvorschriften und unteren Weisungen;
- Unverzügliche Meldung an den Vorgesetzten, wenn in einem Datenschutzfall die Hilfe des Vorgesetzten oder des Datenschutzbeauftragten notwendig ist;
- Teilnahme an Schulungen bezüglich Datenverarbeitung, Datenschutz.

## **5.2. Regeln für Datensicherheit**

Artikel 32 DSGVO festgelegt, dass 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 treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

- die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Zur Sicherheit der auf Papier verarbeiteter personenbezogener Daten wendet die Organisation, im Einklang mit den Vorschriften der geltenden Dokumentenverwaltungsregelung folgende Maßnahmen an:

- nur dazu Befugte dürfen die Daten kennenlernen. Niemand anders hat Zugriff zu ihnen, sie sind keiner anderen Partei aufzudecken;
- die Dokumente müssen in einem gut verschließbaren, trockenem, mit einer Feuerschutz- und Vermögenssicherungsanlage versehenem Raum untergebracht werden;
- nur die Zuständigen haben Zugriff zu den fortlaufend aktiv bearbeiteten Unterlagen;
- die Datenverarbeitung der Organisation durchführende Personen können im Laufe des Tages jene Räumlichkeiten, in denen eine Datenverarbeitung stattfindet, nur so verlassen, dass sie die ihnen anvertraute Datenträger verschließen, oder das Büro schließen;
- die Datenverarbeitung der Organisation durchführenden Arbeitnehmer müssen am Ende der Arbeitsdurchführung die Papier-Datenträger verschließen;
- die Archivierung der in der vorliegenden Regelung bestimmter Akten muss jährlich einmal durchgeführt werden, die archivierten Akten müssen entsprechend der Dokumentenverwaltungsregelung sortiert und in die Archivbearbeitung aufgenommen werden;
- wenn die auf Papier verarbeiteten personenbezogene Daten digitalisiert werden, sind bezüglich der digital gespeicherten Dokumente die Bestimmungen der Regelung für IT-Sicherheit der Organisation maßgebend.

Zur Sicherheit der auf Computer, bzw. dem Netzwerk gespeicherter personenbezogener Daten verwendet die Organisation, im Einklang mit der Regelung für IT-Sicherheit der Organisation folgende Maßnahmen und Garantie-Elemente an:

- die im Laufe der Datenverarbeitung verwendete Computer bilden Eigentum der Organisation, oder die Organisation verfügt über sie mit den Eigentümerrechten identische Rechten;
- man kann auf die sich auf den Computern befindlichen Daten nur mit einer gültigen, personifizierten, identifizierbaren Berechtigung – mit mindestens einem Benutzernamen und einem Passwort – zugreifen, für den Tausch der Passwörter sorgt die Organisation regelmäßig, bzw. in begründeten Fällen;
- die Organisation aufbewahrt und verarbeitet ihre Daten in den Microsoft 365 Cloud-Dienstleistungen. Die Datenaufbewahrung erfolgt in europäischen Zentralen. Microsoft hat die Konformitätserklärungen auf folgender Seite veröffentlicht: <https://servicetrust.microsoft.com/ViewPage/TrustDocumentsV3>
- jeder Computerrecord bezüglich der Daten wird nachverfolgbar geloggt;
- zu den sich auf der Netzwerk Bedienermaschine (im Weiterem: Server) aufbewahrten Daten haben nur über eine geeignete Berechtigung verfügende, und nur die dafür zugewiesenen Personen Zugriff;
- wenn der Zweck der Datenverarbeitung erfüllt worden ist, die Frist der Datenverarbeitung abgelaufen ist, wird die Daten beinhaltende Datei auf eine unwiderrufliche Weise gelöscht, die Daten können nicht wieder zurückgewonnen werden;
- zum Zweck des Vermeidens eines Verlustes der auf dem Netzwerk aufbewahrter Daten führt die Organisation eine ständige Spiegelung auf dem Server durch;
- aus den aktiven Daten der personenbezogenen Daten beinhaltenden Datenbanken wird täglich ein Speichergang durchgeführt, das Speichern bezieht sich auf den gesamten Datenbestand des zentralen Servers, und erfolgt auf einen Magnetdatenträger;
- auf dem personenbezogenen Daten verarbeitenden Netzwerk wird ständig für einen Schutz gegen Viren gesorgt;
- ein Netzwerkszugriff unbefugter Personen wird mit den zur Verfügung stehenden IT-Mitteln, und durch ihre Anwendung verhindert.

## **6. VERLETZUNG DES SCHUTZES PERSONENBEZOGENER DATEN**

### **6.1. Begriff eines Vorfalls der Verletzung des Schutzes personenbezogener Daten im Bereich Datenschutz**

Unter einer Verletzung des Schutzes personenbezogener Daten entsprechend Punkt 12 Artikel 4 der Verordnung, ist eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden. Anhand der Definition kann festgestellt werden, dass ein solcher Sicherheitsvorfall, der der keine personenbezogene Daten betrifft kein Vorfall einer Verletzung des Schutzes personenbezogener Daten darstellt, aber alle Vorfälle der Verletzung des Schutzes personenbezogener Daten stellen einen Sicherheitsvorfall dar.

Die Vorfälle der Verletzung des Schutzes personenbezogener Daten können typischerweise in folgende drei Hauptkategorien eingeteilt werden:

- "Vertraulichkeitsvorfall": rechtswidrige oder zufällige Mitteilung personenbezogener Daten, oder ein unbefugter Zugriff auf sie;
- "Integritätsvorfall": rechtswidrige oder zufällige Veränderung personenbezogener Daten;
- "Erreichbarkeitsvorfall": rechtswidrige oder zufällige Vernichtung personenbezogener Daten, rechtswidriger oder zufälliger Verlust zum Zugriff auf die personenbezogenen Daten.

### **6.2. Handhabung eines Vorfalls der Verletzung des Schutzes personenbezogener Daten**

Jeder Arbeitnehmer der Organisation – darunter verstanden auch die in einem anderen Rechtsverhältnis beschäftigte Personen – sind verpflichtet einen Vorfall der Verletzung des Schutzes personenbezogener Daten innerhalb der Organisation unverzüglich dem Leiter der Organisationseinheit und dem Datenschutzbeauftragten zu melden.

Der Datenschutzbeauftragte fängt nach dem Eintreffen der Meldung unverzüglich mit der Untersuchung und der Bewertung des Vorfalls der Verletzung des Schutzes personenbezogener Daten an. Der Datenschutzbeauftragte untersucht die Anmeldung, und wenn notwendig, holt er von dem Anmelder weitere Informationen bezüglich des Vorfalls ein. Wenn die Bewertung des Vorfalls der Verletzung des Schutzes personenbezogener Daten einer Untersuchung bedarf, führt der Datenschutzbeauftragte mit Einbeziehung der zur Durchführung der Untersuchung notwendiger Mitarbeiter diese durch.

Die Untersuchung muss beinhalten, ob der Vorfall der Verletzung des Schutzes personenbezogener Daten mit einem hohen Risiko bezüglich der Rechte und Verpflichtungen der berechtigten Personen einhergeht, um welche Art von Risiko es sich handelt, und ob eine Benachrichtigung der Betroffenen über den Vorfall notwendig ist.

Risikozuordnung der Vorfälle der Verletzung des Schutzes personenbezogener Daten:

- Niedriges Risiko: der Vorfall hat keine eigentlichen Auswirkungen auf natürliche Personen, oder verursacht ihnen nur geringere Unannehmlichkeiten, die ohne Probleme zu lösen sind.
- Mittleres Risiko: natürliche Personen erfahren bedeutende Unannehmlichkeiten, die aber unter Schwierigkeiten zu lösen sind.
- Hohes Risiko: natürliche Personen erleben bezüglich des Vorfalls bedeutende Folgen, die sie zwar lösen können, aber nur unter sehr großen Schwierigkeiten.
- Sehr hohes Risiko: natürliche Personen erleben bedeutende oder unwiderrufliche Folgen, die sie unter Umständen nicht lösen können.

Sobald der Organisation eine Verletzung des Schutzes personenbezogener Daten bekannt wird, muss die Aufsichtsbehörde von der Verletzung des Schutzes personenbezogener Daten unverzüglich und, falls möglich, binnen höchstens 72 Stunden, nachdem die Verletzung bekannt wurde, unterrichten, es sei denn, der Verantwortliche kann im Einklang mit dem Grundsatz der Rechenschaftspflicht nachweisen, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem

Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen führt. Falls diese Benachrichtigung nicht binnen 72 Stunden erfolgen kann, sollten in ihr die Gründe für die Verzögerung angegeben werden müssen, und die Informationen können schrittweise ohne unangemessene weitere Verzögerung bereitgestellt werden.

Die Meldung enthält zumindest folgende Informationen:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
- den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
- eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
- eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Der für die Verarbeitung Verantwortliche sollte die betroffene Person, ohne einer unbegründeten Verzögerung von der Verletzung des Schutzes personenbezogener Daten benachrichtigen, wenn diese Verletzung des Schutzes personenbezogener Daten voraussichtlich zu einem hohen Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen führt. Der Verantwortliche ist verpflichtet mindestens folgende Informationen der betroffenen Person zu erteilen:

- die Art des Vorfalls der Verletzung des Schutzes personenbezogener Daten;
- den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
- eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
- eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Die Betroffenen müssen nicht benachrichtigt werden, wenn einer der folgenden Bedingungen erfüllt wird:

- der Verantwortliche geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen hat und diese Vorkehrungen auf die von der Verletzung betroffenen personenbezogenen Daten angewandt wurden, insbesondere solche, durch die die personenbezogenen Daten für alle Personen, die nicht zum Zugang zu den personenbezogenen Daten befugt sind, unzugänglich gemacht werden, etwa durch Verschlüsselung;
- der Verantwortliche durch nachfolgende Maßnahmen sichergestellt hat, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Personen aller Wahrscheinlichkeit nach nicht mehr besteht;
- dies mit einem unverhältnismäßigen Aufwand verbunden wäre. In diesem Fall hat stattdessen eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme zu erfolgen, durch die die betroffenen Personen vergleichbar wirksam informiert werden.

### **6.3. Erfassen eines Vorfalls der Verletzung des Schutzes personenbezogener Daten**

Anhand der Vorschriften der DSGVO führt der Datenschutzbeauftragte zur Kontrolle der mit dem Vorfall der Verletzung des Schutzes personenbezogener Daten verbundener Maßnahmen, und der Benachrichtigung der betroffenen Personen ein Verzeichnis, welches Folgendes beinhaltet:

- den Kreis der betroffenen personenbezogenen Daten,
- den Kreis und Anzahl der von dem Vorfall der Verletzung des Schutzes personenbezogener Daten betroffener Personen,

- den Zeitpunkt des Vorfalls der Verletzung des Schutzes personenbezogener Daten,
- die Umstände und Auswirkungen des Vorfalls der Verletzung des Schutzes personenbezogener Daten,
- die zur Behebung des Vorfalls der Verletzung des Schutzes personenbezogener Daten unternommene Maßnahmen,
- die in den die Datenverarbeitung vorschreibenden Rechtsvorschriften definierte weitere Angaben.

Die im Verzeichnis aufgeführte Angaben zu den Vorfällen der Verletzung des Schutzes personenbezogener Daten müssen 5 Jahre lang aufbewahrt werden. Das Arbeitsblatt der zutreffenden Anlage beinhaltet ein Musterverzeichnis für Vorfälle der Verletzung des Schutzes personenbezogener Daten.

## **7. VORSTELLUNG DER FOLGENABSCHÄTZUNG FÜR DATENSCHUTZ, DER VORANGEHENDEN KONSULTATION UND DER INTERESSENABWÄGUNG**

### **7.1. Datenschutz-Folgenabschätzung**

Hat eine neue Form der Datenverarbeitung - aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung - voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt die Organisation vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch. Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden.

Nach der Hauptregel führt der Datenschutzbeauftragte die Folgenabschätzung durch. Wenn dies nicht der Datenschutzbeauftragte tut, so ist die Organisation verpflichtet den fachlichen Rat des Datenschutzbeauftragten einzuholen.

Nach der Durchführung der Folgenabschätzung muss nach Bedarf, aber mindestens bei einer Veränderung der durch die Datenverarbeitungsschritte verursachten Risiken die Folgenabschätzung überprüft werden, und im Laufe dessen muss die Bewertung erneut durchgeführt werden. Die Überprüfung der Risiken muss mindestens alle 3 Jahre stattfinden.

Eine weitere Verpflichtung des Verantwortlichen bezüglich der Verarbeitung personenbezogener Daten ist die Erstellung einer Risikoanalyse, deren Schritte Folgende sind:

- Identifizierung der mit der Verarbeitung personenbezogener Daten verbundener Risiken,
- Erstellen einer Risikoliste,
- Festlegen der wahrscheinlichen Hauptgründe der einzelnen Risiken und der zu erwartenden negativen Folgen und
- anhand dessen das Erarbeiten von präventiven und korrektiven Prozessen der Risikobewältigung.

Ein Aufdecken der Risikoquellen ist notwendig, innerhalb dessen müssen die Elemente der präventiven und korrektiven Zielerreichung festgelegt werden, wie auch das System der Ressourcenverwaltung und die objektiven und subjektiven Risikoelemente müssen voneinander getrennt werden. Im Laufe der Analyse muss ein vollständiges Risikobewertungssystem erarbeitet werden, in dem die Festlegung des gesamten Risikopotentials und einer Prioritätenzuordnung der Risiken (nicht identisch mit dem Maßnahmenplan) stattfinden muss. Der Verlauf und die Ergebnisse der Analyse müssen schriftlich erfasst werden.

Bei dem Risikopotential müssen aus Sicht der Wahrscheinlichkeit Risiken mit einer

- geringen
- mittleren
- hohen Eintrittswahrscheinlichkeit,

und aus Sicht der Tragweite Risiken mit einer

- geringen

- mittleren
- großen Tragweite festgelegt werden.

Diese Festlegung ist die Grundlage eines späteren Verfahrens der Risikobehandlung, sowohl aus Sicht eines präventiven, als auch eines korrekativen Verfahrens. Der Datenschutzbeauftragte ist verantwortlich für die Durchführung der Risikoanalyse.

## **7.2. Vorherige Konsultation**

Wenn die durchgeführte Folgenabschätzung feststellt, dass der Prozess der Datenverarbeitung ein hohes Risiko zu Folge hätte, konsultiert die Organisation vor Beginn des Prozesses der Datenverarbeitung mit der Aufsichtsbehörde.

Die Organisation reicht zur Konsultation Folgendes ein:

- die durchgeführte Datenschutz-Folgenabschätzung,
- den Namen und die Erreichbarkeiten des Datenschutzbeauftragten,
- eine Auflistung der Aufgabenkreise des/der an dem Prozess der Datenverarbeitung beteiligten/r Verantwortlichen, Auftragsverarbeiter,
- den Zweck und die Art der Datenverarbeitung und
- die zum Schutz der der Sicherstellung der Rechte, Freiheiten der Betroffenen unternommene Maßnahmen, Garantien.

## **7.3. Interessenabwägung**

Entsprechend Punkt f) Absatz (1) Artikel 6 der DSGVO besteht die Möglichkeit einer Datenverarbeitung ohne Zustimmung, wenn dies durch ein berechtigtes Interesse ermöglicht wird, angenommen, dass die Organisation, als Verantwortlicher ihre Aufklärungspflichten erfüllt. Wenn die Rechtsgrundlage durch Punkt f) Absatz (1) Artikel 6 der DSGVO gegeben ist, wird der Datenverarbeitungsprozess dann und in dem Ausmaß rechtmäßig, soweit die Datenverarbeitung zur Geltendmachung der berechtigten Interessen des Verantwortlichen oder einer Drittpartei notwendig ist, außer wenn gegenüber diesem Interesse jene Interessen oder grundlegende Rechte und Freiheiten der betroffenen Person Vorrang haben, die den Schutz der personenbezogenen Daten notwendig machen.

Zur Untersuchung der Rechtmäßigkeit der Datenverarbeitung führt die Organisation einen Interessenabwägungstest durch, in Laufe dessen die Notwendigkeit des Zwecks der Datenverarbeitung und die verhältnismäßige Einschränkung der Rechte und Freiheiten der Betroffenen untersucht und entsprechend begründet werden.

Die Organisation identifiziert im Laufe des Interessenabwägungstests ihr berechtigtes Interesse für die Datenverarbeitung, und die den Gegenpol der Gewichtung bildenden Interessen der Betroffenen und die betroffene Rechtsgrundlage. Die Organisation muss die Bedingung der Gewichtung der gegensätzlichen Rechte und Interessen immer unter Berücksichtigung der individuellen Umstände des jeweiligen Falles untersuchen. Im Laufe der Abwägung berücksichtigt die Organisation besonders die Natur der verarbeiteten oder zu verarbeitenden Daten und ihren sensitiven Charakter, die schwere des eventuell stattfindenden Regelverstoßes usw.

Die Organisation führt als Teil des Interessenabwägungstests auch eine Untersuchung der Notwendigkeit und Verhältnismäßigkeit durch, in deren Sinne die Ausnahmefälle des Schutzes der personenbezogenen Daten und die Einschränkung des Schutzes innerhalb der Grenzen des unbedingt notwendigen Ausmaßes bleiben müssen. Die Art und die Menge der zu verarbeitenden Daten darf nicht die zur Geltendmachung berechtigter Interessen notwendige Menge überschreiten. Die Untersuchung der Verhältnismäßigkeit beinhaltet die Bewertung des Verhältnisses zwischen dem Zweck und den ausgewählten Mitteln. Die ausgewählten Mittel dürfen das Maß der Notwendigkeit nicht überschreiten, aber sie müssen auch zum Erreichen des festgelegten Zwecks geeignet sein. Anhand der Durchführung der Gewichtung stellt die Organisation fest, ob die personenbezogenen Daten verarbeitet werden können.

Die Betroffenen werden über das Testergebnis benachrichtigt, woraus eindeutig ersichtlich ist, anhand welcher berechtigten Interessen und weshalb eine Verarbeitung personenbezogener Daten ohne eine Zustimmung durch die Organisation als verhältnismäßige Einschränkung betrachtet werden kann, weshalb also das berechnete Interesse an der Datenverarbeitung die Interessen, bzw. Rechte der Betroffenen übersteigt. Die Organisation informiert die betroffene Person über die unter Berücksichtigung der fehlenden Zustimmung getroffenen Datenschutzgarantien und über die Möglichkeiten der Einwände gegen die Datenverarbeitung. Ein Ergebnis der Gewichtung zwischen den gegensätzlichen Interessen und Rechten kann nicht vorgeschrieben werden, ohne dass die Organisation unter Berücksichtigung der individuellen Gegebenheiten des jeweiligen Falls ein abweichendes Ergebnis ermöglichen würde, deshalb führt die Organisation in jedem einzelnen Fall einen gesonderten Interessenabwägungstest durch.

## **8. GELTENDMACHUNG DER RECHTE DER BETROFFENEN**

### **8.1. Übersichtliche Aufklärung, Kommunikation und Unterstützung der Ausübung der Rechte der Betroffenen**

Die Organisation muss den betroffenen Personen alle Informationen und jede einzelne Aufklärung bezüglich der Verarbeitung ihrer personenbezogenen Daten in einer bündigen, übersichtlichen, verständlichen und leicht erreichbaren Form, klar und verständlich formuliert angeben, besonders bei jeglichen an Kinder adressierter Informationen. Die Informationen müssen schriftlich oder auf eine andere Weise – darunter verstanden auch den elektronischen Weg – angegeben werden. Auf Wunsch der Betroffenen können auch mündliche Auskünfte erteilt werden, angenommen, dass die betroffene Person auf einem anderen Weg identifiziert worden ist.

Die Organisation muss die Ausübung der Rechte der Betroffenen unterstützen.

Die Organisation benachrichtigt die betroffene Person ohne eine begründete Verzögerung, aber auf jeden Fall innerhalb von 30 Tagen ab der Zustellung des Antrages über die in Folge seines Antrages zur Ausübung der Rechte getroffenen Maßnahmen. Diese Frist kann durch die in der Verordnung aufgeführten Bedingungen um weitere 60 Tage verlängert werden, aber der Betroffene muss über die konkreten Gründe der Verzögerung informiert werden.

Wenn die Organisation in Folge des Antrages der betroffenen Person keine Maßnahmen einleitet, informiert sie die betroffene Person ohne eine begründete Verzögerung, aber auf jeden Fall innerhalb von 30 Tagen ab der Zustellung des Antrages über die Gründe des Ausbleibens der Maßnahmen, und darüber, dass eine Beschwerde bei einer Aufsichtsbehörde einreichen werden kann, und von dem Recht eines gerichtlichen Rechtsbehelfes Gebrauch gemacht werden kann.

Der Verantwortliche stellt die Informationen und die Aufklärung bezüglich der Rechte der betroffenen Person und die Maßnahmen kostenlos zur Verfügung, aber in den in der Verordnung aufgeführten Fällen kann eine Gebühr berechnet werden.

Die betroffene Person ist berechtigt, vor Beginn der Datenverarbeitung eine Aufklärung über die Fakten und Informationen bezüglich der Datenverarbeitung zu erhalten. Im Rahmen dessen muss die betroffene Person über folgendes informiert werden:

- die Person und die Erreichbarkeiten des Verantwortlichen und seines Vertreters,
- die Erreichbarkeiten des Datenschutzbeauftragten (wenn es einen gibt),
- den Zweck der geplanten Verarbeitung der personenbezogenen Daten, und der Rechtsgrundlage der Datenverarbeitung,
- bei einer auf der Geltendmachung berechtigter Interessen beruhender Datenverarbeitung, die berechtigten Interessen des Verantwortlichen oder einer Drittpartei,
- den Empfänger der personenbezogenen Daten – jene, denen die Daten bekanntgegeben werden -, bzw. über die Kategorien der Empfänger, wenn es solche gibt;
- gegebenenfalls über die Tatsache, dass der Verantwortliche die personenbezogenen Daten in ein Drittland oder an internationale Organisationen weiterleiten möchte.

Zur Sicherstellung einer nach Treu und Glauben stattfindenden, transparenten Datenverarbeitung muss die Organisation die betroffene Person über folgende ergänzende Informationen benachrichtigen:

- die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
- das Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit;
- wenn die Verarbeitung auf einer Zustimmung des Betroffenen beruht, das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird;
- das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;
- ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche möglichen Folgen die Nichtbereitstellung hätte und
- über das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling, und zumindest in diesen Fällen aussagekräftige Informationen über die involvierte Logik sowie verständliche Informationen über die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person zu Folge hat.

Bezüglich der Verarbeitung von Arbeitnehmerdaten ist als Anlage des Regelwerkes eine Aufklärung für Arbeitnehmer erstellt worden, deren Zweck eine vorangehende Aufklärung der Arbeitnehmer über die Datenverarbeitung ist.

## **8.2. Zugriffrecht der Betroffenen**

Anhand Artikel 15 der DSGVO ist die betroffene Person berechtigt einen Zugriff zu den sich auf sie beziehenden personenbezogenen Daten laut der Folgenden zu verlangen:

(1) Die betroffene Person hat das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat sie ein Recht auf Auskunft über diese personenbezogenen Daten und auf folgende Informationen:

- die Zwecke der Verarbeitung;
- die Kategorien personenbezogener Daten, die verarbeitet werden;
- die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen;
- falls möglich die geplante Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
- das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten oder auf Einschränkung der Verarbeitung durch den Verantwortlichen oder eines Widerspruchsrechts gegen diese Verarbeitung;
- das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;
- wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die Herkunft der Daten;
- das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling, und zumindest in diesen Fällen aussagekräftige Informationen über die involvierte Logik sowie verständliche Informationen über die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person zu Folge hat.

(2) Der Verantwortliche stellt eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung. Für alle weiteren Kopien, die die betroffene Person beantragt, kann der Verantwortliche ein angemessenes Entgelt auf der Grundlage der Verwaltungskosten verlangen.



Stellt die betroffene Person den Antrag elektronisch, so sind die Informationen in einem gängigen elektronischen Format zur Verfügung zu stellen, sofern sie nichts anderes angibt. Das Recht auf Erhalt einer Kopie darf die Rechte und Freiheiten anderer Personen nicht beeinträchtigen.

### **8.3. Recht auf Berichtigung**

Anhand Artikel 16 der DSGVO ist die betroffene Person berechtigt von dem Verantwortlichen eine Berichtigung der sich auf sie beziehenden personenbezogenen Daten zu verlangen:

Im Falle eines Antrages der betroffenen Person ist der Verantwortliche unverzüglich verpflichtet die Berichtigung der betreffenden unrichtigen personenbezogener Daten durchzuführen. Unter Berücksichtigung der Zwecke der Verarbeitung hat die betroffene Person das Recht, die Vervollständigung unvollständiger personenbezogener Daten — auch mittels einer ergänzenden Erklärung — zu verlangen.

Im Falle einer Berichtigung müssen die berichtigten personenbezogenen Daten allen bekanntgegeben werden, denen die ursprünglichen personenbezogenen Daten bekanntgegeben worden waren.

### **8.4. Recht auf Datenlöschung**

Anhand Artikel 17 der DSGVO ist die betroffene Person berechtigt vom Verantwortlichen die Löschung der sich auf sie beziehenden personenbezogenen Daten laut der Folgenden zu verlangen:

(1) Die betroffene Person hat das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, und der Verantwortliche ist verpflichtet, personenbezogene Daten unverzüglich zu löschen, sofern einer der folgenden Gründe zutrifft:

- Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig.
- Die betroffene Person widerruft ihre Einwilligung, auf die sich die Verarbeitung stützte, und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung;
- Die betroffene Person legt Widerspruch gegen die Verarbeitung aus öffentlichem Interesse, der Ausübung der öffentlichen Gewalt oder dem berechtigten Interesse des Auftragsverarbeiters (Drittpartei) ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor, oder die betroffene Person legt Widerspruch gegen die Verarbeitung zum Zwecke einer Direktwerbung;
- Die personenbezogenen Daten wurden unrechtmäßig verarbeitet.
- Die Löschung der personenbezogenen Daten ist zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten (dem ungarischen Recht) erforderlich, dem der Verantwortliche unterliegt.
- Die personenbezogenen Daten wurden in Bezug auf angebotene Dienste der Informationsgesellschaft erhoben.

(2) Hat der Verantwortliche die personenbezogenen Daten öffentlich gemacht und ist er gemäß Absatz 1 zu deren Löschung verpflichtet, so trifft er unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten angemessene Maßnahmen, auch technischer Art, um für die Datenverarbeitung Verantwortliche, die die personenbezogenen Daten verarbeiten, darüber zu informieren, dass eine betroffene Person von ihnen die Löschung aller Links zu diesen personenbezogenen Daten oder von Kopien oder Replikationen dieser personenbezogenen Daten verlangt hat.

(3) Eine Einschränkung des Rechtes auf Löschung der betroffenen Personen kann nur im Falle des Bestehens einer der in der DSGVO aufgeführten Ausnahmen erfolgen, also beim Bestehen der oben aufgeführten Gründe kann eine Aufbewahrung der personenbezogenen Daten als rechtmäßig betrachtet werden, wenn dies aus einer der folgenden Gründe notwendig ist:

- zur Ausübung des Rechts auf freie Meinungsäußerung und Information, oder

- zur Erfüllung einer rechtlichen Verpflichtung, oder
- zur Durchführung einer Aufgabe aus öffentlichen Interessen, oder
- zur Ausübung öffentlicher Gewalt, die dem Verantwortlichen übertragen wurde, oder
- aus öffentlichem Interesse, der den Bereich der öffentlichen Gesundheit betrifft,
- für im öffentlichen Interesse liegende Archivzwecke, oder
- für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke, oder
- zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

Eine wichtige Verpflichtung bezüglich der Löschung ist auch, dass die verarbeiteten personenbezogenen Daten durch all jene gelöscht werden müssen, die über die Organisation Zugriff zu den personenbezogenen Daten erlangt haben.

## **8.5. Recht auf Einschränkung der Verarbeitung**

Anhand Artikel 18 der DSGVO ist die betroffene Person berechtigt vom Verantwortlichen die Einschränkung der sich auf sie beziehenden personenbezogenen Daten laut der Folgenden zu verlangen:

(1) Die betroffene Person hat das Recht, von dem Verantwortlichen die Einschränkung der Verarbeitung zu verlangen, wenn eine der folgenden Voraussetzungen gegeben ist:

- die Richtigkeit der personenbezogenen Daten von der betroffenen Person bestritten wird, und zwar für eine Dauer, die es dem Verantwortlichen ermöglicht, die Richtigkeit der personenbezogenen Daten zu überprüfen,
- die Verarbeitung unrechtmäßig ist und die betroffene Person die Löschung der personenbezogenen Daten ablehnt und stattdessen die Einschränkung der Nutzung der personenbezogenen Daten verlangt;
- der Verantwortliche die personenbezogenen Daten für die Zwecke der Verarbeitung nicht länger benötigt, die betroffene Person sie jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt, oder
- die betroffene Person Widerspruch gegen die Verarbeitung aus öffentlichem Interesse, der Ausübung der öffentlichen Gewalt oder dem berechtigten Interesse des Auftragsverarbeiters (Drittpartei) eingelegt hat, solange noch nicht feststeht, ob die berechtigten Gründe des Verantwortlichen gegenüber denen der betroffenen Person überwiegen.

(2) Wurde die Verarbeitung gemäß der oben Beschriebenen eingeschränkt, so dürfen diese personenbezogenen Daten — von ihrer Speicherung abgesehen — nur mit Einwilligung der betroffenen Person oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder zum Schutz der Rechte einer anderen natürlichen oder juristischen Person oder aus Gründen eines wichtigen öffentlichen Interesses der Union oder eines Mitgliedstaats verarbeitet werden.

(3) Eine betroffene Person, die eine Einschränkung der Verarbeitung gemäß Absatz 1 erwirkt hat, wird von dem Verantwortlichen unterrichtet, bevor die Einschränkung aufgehoben wird.

Die betroffene Person muss über das Aufheben der Einschränkung im Voraus benachrichtigt werden.

## **8.6. Recht auf Datenübertragbarkeit**

Anhand Artikel 20 der DSGVO ist die betroffene Person zur Datenübertragbarkeit der sich auf sie beziehenden personenbezogenen Daten laut der Folgenden berechtigt:

(1) Die betroffene Person hat das Recht, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, und sie hat das Recht, diese Daten einem anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, dem die personenbezogenen Daten bereitgestellt wurden, zu übermitteln, sofern

- wenn die Rechtsgrundlage der Datenverarbeitung eine Zustimmung der betroffenen Person, oder die Erfüllung eines mit der betroffenen Person abgeschlossenen Vertrages ist
- und die Verarbeitung mithilfe automatisierter Verfahren erfolgt.

(2) Bei der Ausübung ihres Rechts auf Datenübertragbarkeit hat die betroffene Person das Recht, zu erwirken, dass die personenbezogenen Daten direkt von einem Verantwortlichen einem anderen Verantwortlichen übermittelt werden, soweit dies technisch machbar ist.

(3) Die Ausübung des Rechts auf Datenübertragbarkeit lässt das Recht auf Löschen unberührt. Dieses Recht gilt nicht für eine Verarbeitung, die für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde.

(4) Das Recht auf Datenübertragbarkeit darf die Rechte und Freiheiten anderer Personen nicht beeinträchtigen.

Die Ausübung des Rechts auf Datenübertragbarkeit lässt Artikel 17 der Verordnung unberührt (Recht auf Löschen („Recht auf Vergessenwerden“)). Das Recht auf Datenübertragbarkeit gilt nicht für eine Verarbeitung, die für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Dieses Recht darf die Rechte und Freiheiten anderer Personen nicht beeinträchtigen

## **8.7. Widerspruchsrecht**

Anhand Artikel 21 der DSGVO ist die betroffene Person berechtigt vom Verantwortlichen gegen die Verarbeitung der sich auf sie beziehenden personenbezogenen Daten laut der Folgenden Widerspruch einzulegen:

(1) Die betroffene Person hat das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten, die aufgrund eines öffentlichen Interesses, der Ausübung öffentlicher Gewalt oder dem berechtigten Interesse des Auftragsverarbeiters (Drittpartei) erfolgt, Widerspruch einzulegen; dies gilt auch für ein auf diese Bestimmungen gestütztes Profiling. Der Verantwortliche verarbeitet die personenbezogenen Daten nicht mehr, es sei denn, er kann zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

(2) Werden personenbezogene Daten verarbeitet, um Direktwerbung zu betreiben, so hat die betroffene Person das Recht, jederzeit Widerspruch gegen die Verarbeitung sie betreffender personenbezogener Daten zum Zwecke derartiger Werbung einzulegen; dies gilt auch für das Profiling, soweit es mit solcher Direktwerbung in Verbindung steht. Widerspricht die betroffene Person der Verarbeitung für Zwecke der Direktwerbung, so werden die personenbezogenen Daten nicht mehr für diese Zwecke verarbeitet.

(3) Die betroffene Person muss spätestens zum Zeitpunkt der ersten Kommunikation mit ihr ausdrücklich auf das Widerspruchsrecht hingewiesen werden; dieser Hinweis hat in einer verständlichen und von anderen Informationen getrennten Form zu erfolgen.

(4) Im Zusammenhang mit der Nutzung von Diensten der Informationsgesellschaft kann die betroffene Person ungeachtet der Richtlinie 2002/58/EG ihr Widerspruchsrecht mittels automatisierter Verfahren ausüben, bei denen technische Spezifikationen verwendet werden.

(5) Die betroffene Person hat das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, gegen die sie betreffende Verarbeitung sie betreffender personenbezogener Daten, die zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken erfolgt, Widerspruch einzulegen, es sei denn, die Verarbeitung ist zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe erforderlich.

## **8.8. Automatisierte Entscheidungen im Einzelfall einschließlich Profiling**

Die betroffene Person hat das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung — einschließlich Profiling — beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet, oder sie in ähnlicher Weise erheblich beeinträchtigt.

Diese Berechtigung ist nicht anzuwenden, wenn die Entscheidung:

- für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und der Organisation erforderlich ist,
- aufgrund von Rechtsvorschriften der Union oder der Mitgliedstaaten, denen die Organisation unterliegt, zulässig ist und diese Rechtsvorschriften angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten oder
- mit ausdrücklicher Einwilligung der betroffenen Person erfolgt.

## **8.9. Recht auf Rechtsbehelf**

Jede betroffene Person hat das Recht auf Beschwerde bei einer Aufsichtsbehörde, insbesondere in dem Mitgliedstaat ihres Aufenthaltsorts, ihres Arbeitsplatzes oder des Orts des mutmaßlichen Verstoßes, wenn die betroffene Person der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen diese Verordnung verstößt. Die Aufsichtsbehörde, bei der die Beschwerde eingereicht wurde, unterrichtet den Beschwerdeführer über den Stand und die Ergebnisse der Beschwerde einschließlich der Möglichkeit eines gerichtlichen Rechtsbehelfs.

### **Nemzeti Adatvédelmi és Információszabadság Hatóság**

**(Nationale Behörde für Datenschutz und Informationsfreiheit)**

**Postadresse: 1363 Budapest, Pf.: 9.**

**Adresse: 1055 Budapest, Falk Miksa utca 9-1 1.**

**Telefon: +36 (1) 391-1400**

**Fax: +36 (1) 391-1410**

**E-Mail: ugyfelszolgalat (At-Zeichen) [naih.hu](mailto:naih.hu)**

Jede natürliche oder juristische Person hat unbeschadet eines anderweitigen verwaltungsrechtlichen oder außergerichtlichen Rechtsbehelfs das Recht auf einen wirksamen gerichtlichen Rechtsbehelf gegen einen sie betreffenden rechtsverbindlichen Beschluss einer Aufsichtsbehörde. Jede betroffene Person hat unbeschadet eines anderweitigen verwaltungsrechtlichen oder außergerichtlichen Rechtsbehelfs das Recht auf einen wirksamen gerichtlichen Rechtsbehelf, wenn die zuständige Aufsichtsbehörde sich nicht mit einer Beschwerde befasst oder die betroffene Person nicht innerhalb von drei Monaten über den Stand oder das Ergebnis der erhobenen Beschwerde in Kenntnis gesetzt hat.

Jede betroffene Person hat unbeschadet eines verfügbaren verwaltungsrechtlichen oder außergerichtlichen Rechtsbehelfs einschließlich des Rechts auf Beschwerde bei einer Aufsichtsbehörde das Recht auf einen wirksamen gerichtlichen Rechtsbehelf, wenn sie der Ansicht ist, dass die ihr aufgrund dieser Verordnung zustehenden Rechte infolge einer nicht im Einklang mit dieser Verordnung stehenden Verarbeitung ihrer personenbezogenen Daten verletzt wurden. Ein Verfahren gegenüber dem Verantwortlichen oder dem Auftragsverarbeiter muss vor dem Gericht des Mitgliedsstaates des Tätigkeitsortes des Verantwortlichen oder des Auftragsverarbeiters eingeleitet werden. So ein Verfahren kann auch vor dem Gericht des Mitgliedsstaates des üblichen Aufenthaltsortes der betroffenen Person eingeleitet werden, dies gilt nicht, wenn es sich bei dem Verantwortlichen oder dem Auftragsverarbeiter um eine Behörde eines Mitgliedstaats handelt, die in Ausübung ihrer hoheitlichen Befugnisse tätig geworden ist.

## **9. SCHLUSSBESTIMMUNGEN**

Die vorliegende Regelung tritt am 28. Mai 2021 in Kraft.

Das Kennenlernen des Inhaltes der Regelung und das Einhalten ihrer Vorschriften gehört zu den Arbeitsplatzpflichten der Arbeitnehmer der Organisation, für die Vertragspartner der Organisation ist in Abhängigkeit der sich auf sie beziehenden Vertragsvorschriften, dies eine Vertragspflicht.

Eine Veränderung einer der Anlagen zieht nicht eine Modifizierungspflicht der vorliegenden Regelung mit sich.

## **10. ANLAGEN**

Anlage Nr. 1: Geheimhaltungserklärung

Anlage Nr. 2: Datenschutzaufklärung für Arbeitnehmer

Anlage Nr. 3: Zustimmungserklärung zum Erstellen von Bildern und Videoaufnahmen

Anlage Nr. 4: Antwortbriefmuster für eingereichte Lebensläufe

Anlage Nr. 5: Test für Interessenabwägung im Bereich Datenschutz

Anlage Nr. 6: Wegweiser zum Erstellen der Datenschutz Folgenabschätzung

Anlage Nr. 7: Verzeichnis für Vorfälle der Verletzung des Schutzes personenbezogener Daten

Datiert: Veszprém, den 28. Mai 2021

*[unleserliche Unterschrift]*

Aliz Markovits

Generaldirektorin

*[Stempel:]*

*Veszprém-Balaton 2023 Zrt.  
8200 Veszprém, Óváros tér 26.  
FirmenregNr.: 19-10-500277  
Steuernummer: 23701142-2-19*

2.