indivizo+

# Adatbiztonsági Szabályzat

Szabályzat Indivizo munkavállalói és alvállalkozói (innentől *munkatársak*) számára a munkavégzés során alkalmazandó adatbiztonsági gyakorlatról.

## Általános rendelkezések

1. Indivizo rendszerében kezelt felhasználói és ügyfél adatok üzleti titoknak minősülnek, melyek kezelésére érvényesek a munkatárssal megkötött munkaszerződés illetve alvállalkozói szerződés és adatfeldolgozói szerződés rendelkezései.
2. Munkatársak kötelesek a munkájuk során kezelt adatokat a tőlük telhető legnagyobb biztonsággal, de legalább a jelen szabályzat által meghatározott módon kezelni.
3. Jelen szabályzat Indivizo által bármikor egyoldalúan módosítható.

## Személyi számítógép védelme

Munkatársak kötelesek a munkavégzésre használt személyi számítógépek szoftveres és fizikai védelméről gondoskodni:

1. Rendszeres vírus kereséssel és írtással;
2. A számítógép merevlemezének titkosításával (pl.: FileValut, BitLocker);
3. A számítógépet csak lezárva hagyja felügyelet nélkül;
4. Szervízelés előtt minden munkavégzés során használt adatot fizikai törléssel el kell távolítani a merevlemezről, vagy a merevlemezt kell eltávolítani a számítógépből;
5. Munkavégzés során csak megbízható, jelszóval védett hálózatról csatlakozik az internetre, szükség esetén VPN használatával.
6. A merevlemez rendszeres biztonsági mentése esetén gondoskodni kell a mentés titkosításáról, illetve az abban tárolt adatok törléséről, amikor azokra már nincs szükség.

indivizo+

# Data Security Policy

Policy on the data security practices to be applied by the employees and subcontractors (hereinafter: '*associates*') of Indivizo during the performance of their work.

## General provisions

1. The user and customer data processed in Indivizo's system are classified as business secrets and are governed by the terms and conditions of the employment contract concluded with the associate, the subcontracting agreement and the data processing contract.
2. Associates are obligated to process the data processed by them during their work with the greatest possible security, but at least in the manner prescribed by this Policy.
3. This Policy may be amended unilaterally by Indivizo at any time.

## Personal computer protection

Associates are required to ensure software and physical protection for personal computers used for work:

1. With regular virus scanning and debugging;
2. With the encryption of their computer's hard drive (e.g.: FileValut, BitLocker);
3. By leaving the computer unattended only when locked;
4. By removing all data used during their work before servicing, either by physical erasure or by removing the hard drive from the computer;
5. By only connecting to the Internet from a trusted, password-protected network while working, using a VPN if necessary.
6. During the regular back up of the hard drive it should be ensured that the backup is encrypted and that the data stored in it is erased when it is no longer required.

indivizo+

# Adatbiztonsági Szabályzat

## Felhasználói adatok kezelése

1. A munkatársak csak és kizárólag a feladatuk elvégzése céljából kérdezhetnek le és használhatnak felhasználói adatokat.
2. Amennyiben az adott feladat elvégezhető a felhasználói adatok nélkül, úgy a feladatot ilyen módon kell végrehajtani.
3. A feladat elvégzése után az adatokat törölni kell minden személyes adathordozóról (amennyiben azokat le kellett tárolni a feladat elvégzéséhez).
4. Amennyiben a felhasználói adatokat adathordozóra kell kimenteni, gondoskodni kell annak titkosításáról.

## Felhasználói adatok használata a fejlesztési folyamat során

Indivizo által fejlesztett és üzemeltetett szoftverek fejlesztése során munkavállalók kizárólag az alábbi esetekben használhatják az éles adatbázis másolatát:

1. Olyan hiba felderítése és javítása során, mely nem reprodukálható más módon és adatokkal, csak az éles rendszeren;
2. Olyan változtatás tesztelése során, mely nagy mértékben módosítja a már meglévő adatok struktúráját, így indokolt a kiadás előtt ily módon is ellenőrizni, hogy az adatok migrációja megfelelően fog-e végbemenni.

Fejlesztés során éles adatbázis másolat csak a következő módon használható:

1. A feladathoz nem a valós adatbázis, csak annak másolata használható
2. A másolatban tárolt felhasználó adatokat programozott módon el kell maszkolni, legalább a következők szerint:
    a. Email cím és telefonszám megváltoztatása, hogy a felhasználók ne kaphassanak téves értesítéseket;

indivizo+

# Data Security Policy

## Processing of user data

1. The associates may only query and use user data for the sole purpose of performing their tasks.
2. If the task can be performed without user data, then the task must be performed in such a manner.
3. After completing the task, the data must be erased from all personal media (if they had to be stored to perform the task).
4. If user data is to be saved on a data carrier, encryption should be ensured.

## Use of user data during the development process

When developing software developed and operated by Indivizo, associates may only use a copy of the live database in the following cases:

1. Detecting and correcting an error that cannot be reproduced by other means and with other data, only on the live system;
2. When testing a change that greatly modifies the structure of the existing data, therefore it is appropriate to verify before the release that the migration of the data will take place correctly.

During development, a live database copy can only be used in the following ways:

1. The real database cannot be used for the performance of the task, it may only be a copy thereof
2. The user data stored in the copy must be masked in a programmed manner, at least as follows:
    a. Change e-mail addresses and phone numbers to prevent users from receiving incorrect notifications;