Pacont Kft.

Adatvédelmi szabályzat / Integrity policy

1 Definíció - Definitions

Az adatvédelmi szabályzat meghatározza a Pacont kft. (későbbiekben ”Pacont” vagy ”Társaság”) adatkezelését.

The integrity policy indicates how Pacont (hereinafter “Pacont” or “Company”) shall deal with personal data.

A GDPR (Európai Unió Általános Adatvédelmi Rendelet), ami 2018. május 25-én lép életbe meghatározza, hogy az EU-s tagállamokban működő vállalkozások, így társaságunk is miként kell, hogy kezeljék az adatokat. Az adatvédelmi szabályzat ezt hivatott meghatározni.

The integrity policy is updated with this document to cover requirements in EU’s GDPR, valid from 2018-05-25.

Az adatvédelmi szabályzat a társaság székhelyén érhető el.

The integrity policy shall be kept available at the seat of the Company.

2 Meghatározások - Description

A Társaság csak olyan minimális mennyiségű személyes adatot kezel, amelyek az üzletmenethez feltétlenül szükségesek; csak addig, amíg szükség van rájuk és amennyit a vonatkozó jogszabályok előírnak.

Pacont shall register as few personal data as possible, and only when needed for its operations or to follow legal requirements.

Amennyiben valamilyen személyes adatra nincs már szükség, akkor meg kell semmisíteni.

Personal data no longer needed shall be discarded.

Érzékeny személyes adatok (”tiltott adat”, mint pl. faji megkülönböztetés, politikai nézet, nemi hovatartozás) nem kezelhető/tárolható.

Sensitive personal data (”forbidden information”; e.g. about race, political views, biometry) shall not be registered.

A személyes adatok csak azon alkalmazottak számára hozzáférhetőek, akik azok kezelésével megbízottak és a munkaköri szerepkörük azt megengedi.

Personal data shall only be accessible for an employee who needs them in his or her company functional role.

Kockázat minimalizálás: csak azoknak az alkalmazottaknak van hozzáférésük a személyes adatokhoz, akiknek az jogosultan szükséges. Hordozható, tárgyi anyagok, mint például laptop, ami szenzitív adatok tartalmaz nem vihető az irodán kívülre. VPN-kapcsolatokat minimalizálni szükséges. Laptop, ami bérlőhöz/partnerhez bemutató céljából kikerül nem tartalmazhat szenzitív adatot.

Risk minimalisation: only employees who have a valid need shall have access to personal data. Material, e.g. laptop with potentially sensitive information shall not be brought outside the offices. VPN-connections shall be minimised. Laptop which must be brought to customer for demo or problem solving shall not contain sensitive information.

A munkavégzés helye a Társaság irodája.

Work shall be done in the office.

Amennyiben adatvesztés/szivárgás történik vagy számítógép, ill. egyéb hordozható készülék, ami tartalmaz személyes adatot eltűnik azonnal jelenteni szükséges. Személyes adat, ami ahhoz szükséges, hogy

Data leakage must be reported immediately. Laptop or mobile device which disappears must be reported immediately. Personal data in addition to what is needed to contact users or suppliers shall not be kept on mobile

a partnerekkel (vevő, szállító) kapcsolatba lépjünk nem tárolható mobil egységen.

device.

A jelentés végpontja minden esetben az ügyvezető igazgató és az ő döntési jogköre, hogy az az illetékes hatóság felé továbbításra kerül-e 72 órán belül (Nemzeti Adatvédelmi és Információszabadság Hatóság – NAIH).

Reporting to MD who decides whether reporting to the Authority - NAIH (within 72 hours) is required.

Alkalmazottak: a munkavállalók személyes adatai a Társaság szerverétől függetlenül tartandók (másik gép, papír alapú dokumentumok, mint pl. önéletrajz).

Employees: personal data about employees shall be kept away from the company's server (other computer, paper behind locks, e.g. CV).

Betegség esetén az a közvetlen felettesnek, az ügyvezető igazgatónak jelentendő és nem továbbítandó arra nem illetékes személyeknek.

Sickness shall be reported only to direct leader, to MD, and to the HR function, and shall not be forwarded.

Vevő adatok: csak olyan személyes adatok (név, telefon, e-mail cím) tárolhatóak, melyek az üzletmenethez, munkavégzéshez szükségesek.

Customer information: Pacont shall only store personal data comparising name, employer (customer), phone number, and email address, needed to contact customer or user for work related issues.

A már nem szükséges adatok nem tárolandóak, ill. azokat meg kell semmisíteni, amennyiben azokra már nincs szükség.

Information not needed for our operations (e.g. a user's Person number) shall not be stored, or be destroyed when the need disappears (e.g. food preferences).

Csak olyan fotók tárolhatóak, amelyek szintén az üzletmenetet ill. marketing célokat szolgálnak.

Photos needed for the operations or for marketing may be saved.

Ahhoz, hogy az adat tárolható legyen indokolt ok szükséges (mint pl. partnerek adatai szükségesek a munkavégzéshez/üzletmenet folytatásához, bérleti vagy egyéb jogviszony létesítéséhez), ill. jogilag alátámasztottnak kell lennie (a kapcsolat kialakítás, fenntartás érdekében meghatározott adatok szükségesek).

Such information is stored with the legal ground Approval (Pacont has received the contact information in order to do its job), or Justified interest (we must be able to contact our tenants).

A vevő lista nem menthető mobil egységre, csak azon részek, amelyekre az alkalmazottaknak szükségük van, hogy kapcsolatba tudjanak lépni az ügyfelekkel.

The complete customer list must not be saved on mobile unit; only what the employee needs to contact persons he or she regularly relate with.

Szállítók: csak olyan adat tárolható, ami a beszerzés, szolgáltatás igénybevétel és a fizetéshez szükséges. A kapcsolattartó személyekkel kapcsolatos adatokat érintő részletek azonosak a vevői oldalon ismertetettekkel (lásd feljebb).

Suppliers: only information about the supplier as a company needed for procurement and payment shall be stored. Information about contact persons shall be limited as for users (above).

Dátum: 2018. május 9.

Date: May 9, 2018