Adatkezelési tájékoztató / Privacy notice

eSzemélyiM mobilalkalmazás

1. Adatkezelő megnevezése

Belügyminisztérium

Székhely: 1051 Budapest, József Attila utca 2-4.
Postacím: 1530 Budapest, Pf.: 5
Telefon: + 36 1 441-1000
Fax: + 36 1 441-1437
E-mail cím: ugyfelszolgalat@bm.gov.hu

2. Adatfeldolgozó megnevezése

IdomSoft Informatikai Zrt.

Székhely: 1138 Budapest, Váci út 133.

3. Az adatvédelmi tisztviselő neve és elérhetősége

A Belügyminisztérium adatvédelmi tisztviselője: dr. Tarczi-Ábrahám Dominika
E-mail-címe: adatvedelem@bm.gov.hu

4. Az adatkezelés célja és jogalapja

Az eSzemélyiM mobil alkalmazás olyan kártyakezelő alkalmazás, amely az eSzemélyin tárolt személyes adatok olvasását biztosítja a felhasználók (kártyabirtokosok) részére, valamint támogatja az eSzemélyihez kapcsolódó azonosítók (PIN és PUK kódok) kezelését.

Az alkalmazás használata révén jelennek meg a kiolvasás során az erre használt eszközön, az alábbiakban részletezett adatkezelésben érintett adatok. Az alkalmazás regisztrációhoz kötötten tudja biztosítani a tárolt adatok kiolvasásához a mobileszköz és a kártya összetartozását.

Az alkalmazás felhasználói szerződése, valamint a regisztrációról szóló tájékoztató leírás megtalálható az eszemelyi.hu weboldalon.

4.1 Az eSzemélyi chipjében tárolt adatok kezelése

A személyazonosító igazolvány kiadása és az egységes arcképmás- és aláírás-felvételezés szabályairól szóló 414/2015. (XII. 23.) Korm. rendelet 48. §-a alapján a polgár **a tároló elem tartalmát** a járási hivatalnál, a kijelölt kormányhivatalnál vagy a nyilvántartást kezelő szervnél személyesen, vagy **elektronikus azonosítást követően elektronikus úton ellenőrizheti.**

A fentiekre tekintettel az érintett választhatja azt, hogy az eSzemélyi okmányában tárolt adatokat elektronikus azonosítást követően elektronikus úton ellenőrzi.

Adatkezelés célja	Az elektronikus személyazonosító igazolvány (eSzemélyi) tároló elemén lévő adatok olvasása és azok megjelenítése.
Adatkezelés jogalapja	Az adatkezelés a GDPR 6. cikk (1) bekezdés e) pontján, valamint a személyazonosító igazolvány kiadása és az egységes arcképmás- és aláírás-felvételezés szabályairól szóló 414/2015. (XII. 23.) Korm. rendelet 48. §-án alapul.
Érintett	Az a személy, aki a személyazonosító igazolványának tároló eleméből a saját adatait kiolvasni jogosult
Kezelt adatok köre / tároló elemből kiolvasható adatok	– okmányazonosító – lejárat dátuma és kiállítás kelte – születési név – születési idő – születési hely – neme – viselt családi és utónév – anyja születési neve – személyi azonosító – TAJ szám – adóazonosító jel – lakóhely – tartózkodási hely – külföldi cím – vészhelyzet esetén értesítendő telefonszám – állampolgárság
Adatkezelés időtartama	A felületen történő megjelenítésig

Az alkalmazás gyorsabb futása és annak kényelmesebb használata érdekében az alkalmazás a felhasználó választása szerint képes egy darab CAN szám tárolására, amely a tároló elemben rögzített adatokhoz történő jogszerű hozzáférést biztosító protokoll elindításához szükséges kódszám.

A CAN szám az alábbi feltételekkel kerül tárolásra az alkalmazásban:

- az aktuálisan beírt CAN szám az alkalmazás folyamatos használata mellett 30 percig kerül tárolásra,
- az alkalmazás bezárásával a CAN szám törlésre kerül;
- amennyiben az alkalmazás egy másik CAN számmal rendelkező kártyát érzékel, a CAN szám szintén törlésre kerül.

4.2 Regisztráció során kezelt adatok

Az alkalmazás **személyes adatokat olvas ki a kártyából**, viszont ezek közül kizárólag a regisztrált személy **okmányazonosítóját** tárolja a háttérrendszerében, amely alapján a regisztrált személy közvetve azonosítható. Az okmányazonosító mellett az alkalmazás a kártya **korlátozott azonosítóját** (RID), illetve a készülék **egyedi azonosítóját** is tárolja, amelyek anonim adatnak minősülnek.

A kártya tároló elemében rögzített személyes adatok kezelésére az eAzonosítás funkció használatával kerül sor. Ezen funkció használatához a felhasználónak rendelkeznie kell egy eAzonosítás PIN kóddal, amelyet a kártya első használatba vételekor aktiválni szükséges. Ezt követően van lehetőség regisztrálni. **A regisztráció biztosítja**, hogy a felhasználó a saját eSzemélyi kártyáját összepárosítsa a mobil eszközével. Az összepárosítással a felhasználó a saját kártyájáról bármennyi alkalommal ki tudja olvasni az adatokat, de más, a mobil eszközzel nem párosított kártyá(k)ról összesen 10 alkalommal. Az eSzemélyi birtokosának **hozzájárulását követően** (eAzonosítás PIN kód megadása), az olvasási folyamat során az alkalmazás az eID szervertől lekérdezi a felhasználó adat-megismerési jogosultságát és adathozzáférés-igényeit. Az alkalmazás az eAzonosítás PIN kódot felhasználva felépíti a kártyával a titkosított rádiós csatornát, és elküldi a kártyának a szerver által jóváhagyott műveletek listáját. Ezt a kártya a tranzakció idejéig megjegyzi. Sikeres csatorna-felépítés esetén az alkalmazás „közvetítő" szerepet tölt be az eID szerver és a kártya között. A szerver az alkalmazás nevében azonosítja magát a kártya felé.

Sikeres azonosítás után az eID szerver ellenőrzi az okmány érvényességi státuszát, valamint az abban foglalt adatok helyességét. Ezt követően végrehajtja a kapott kérelem alapján az engedélyezett olvasási műveleteket. **A kártya csak olyan műveletek végrehajtását engedélyezi, amelyekhez az alkalmazásnak joga van, és amelyekhez a felhasználó a beleegyezését adta.** (Amennyiben a chipben tárolt lakcímadatok tekintetében eltérést tapasztal a személyiadat- és lakcímnyilvántartásban tárolt adatokhoz képest, azt jelzi az alkalmazás felé, amely a következő üzenetet jeleníti meg: *„A chipben tárolt lakóhely/tartózkodási hely/külföldi cím nem egyezik meg a személyiadat- és lakcímnyilvántartásban tárolttal.")*

Az eID szerver jelzi a művelet sikeres befejezését az alkalmazás felé és átadja a titkosított válasz azon részét, amelyet a felhasználó ilyen módon kért. Az alkalmazás a kapott választ megjeleníti a felületen a felhasználónak.

Adatkezelés célja	Az elektronikus személyazonosító igazolvány (eSzemélyi) tároló elemén lévő adatok olvasásához az érintett által regisztrált okmány azonosítása
Adatkezelés jogalapja	Az adatkezelés a GDPR 6. cikk (1) bekezdés e) pontján alapul (az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges)
Érintett	az eSzemélyi birtokosa
Kezelt adatok köre	– okmányazonosító – korlátozott azonosító (RID) – készülék egyedi azonosítója

Adatkezelés időtartama	Az okmány érvényességi ideje

5. Az adatkezeléssel kapcsolatos érintetti jogok

5.1. Az adatkezeléssel kapcsolatos érintetti jogok az eSzemélyi chipjében tárolt adatokkal kapcsolatban

5.1.2. A hozzáféréshez való jog

Az Adatkezelő a GDPR Preambulum 63 pontja alapján az érintett számára távoli hozzáférést biztosíthat egy biztonságos rendszerhez, amelyen keresztül az érintett a saját személyes adataihoz közvetlenül hozzáférhet. Ez a jog nem érintheti hátrányosan mások jogait és szabadságait, beleértve az üzleti titkokat vagy a szellemi tulajdont, és különösen a szoftverek védelmét biztosító szerzői jogokat.

5.1.3. A helyesbítéshez való jog

Amennyiben az érintett személy a tárolt adatok kiolvasása során azt tapasztalja, hogy a vészhelyzet esetén értesítendő telefonszám adata nem pontos, ezen adatát azonosítást követően elektronikus úton, a magyarorszag.hu oldalán javíthatja. Egyéb adatai pontatlansága esetén a személyazonosító igazolvány kiadása és az egységes arcképmás- és aláírás-felvételezés szabályairól szóló 414/2015. (XII. 23.) Korm. rendelet 3. §-a alapján, személyes ügyintézés során kérheti adatainak helyesbítését, amennyiben az érintett hitelt érdemlően igazolni tudja a helyesbített adat pontosságát.

5.1.4. Az adatkezelés korlátozásához való jog

Az érintett személy az 5.1.3. pontban megadott, a személyes ügyintézéshez használt elérhetőségeken keresztül kérheti, hogy a személyes adatai kezelését a Belügyminisztérium korlátozza (az adatkezelés korlátozott jellegének egyértelmű jelölésével és az egyéb adatoktól elkülönített kezelés biztosításával) amennyiben

- vitatja a személyes adatai pontosságát (ebben az esetben a Belügyminisztérium arra az időtartamra korlátozza az adatkezelést, amíg ellenőrzi a személyes adatok pontosságát);
- az adatkezelés jogellenes, és az érintett ellenzi az adatok törlését, és ehelyett kéri azok felhasználásának korlátozását;
- az adatkezelőnek már nincs szüksége a személyes adatokra adatkezelés céljából, de az érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez; vagy
- az érintett tiltakozott az adatkezelés ellen (ez esetben a korlátozás arra az időtartamra vonatkozik, amíg megállapításra nem kerül, hogy az adatkezelő jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben).

Az érintett közvetlenül is gyakorolhatja ezen jogát, amennyiben nem ad hozzáférést (PIN kód) az adatai megismeréséhez.

5.1.5. A tiltakozáshoz való jog

Az érintett személy az 1. pontban megadott elérhetőségeken keresztül saját helyzetével kapcsolatos okokból bármikor tiltakozhat az adatkezelés ellen, ha álláspontja szerint a Belügyminisztérium a személyes adatát a jelen adatkezelési tájékoztatóban megjelölt céllal összefüggésben nem megfelelően kezelné. Ebben az esetben a Belügyminisztériumnak kell igazolnia, hogy a személyes adat kezelését olyan kényszerítő erejű jogos okok indokolják, amelyek elsőbbséget élveznek az érintett érdekeivel, jogaival és szabadságaival szemben, vagy amelyek jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódnak.

5.1.6. A törléshez való jog

A tájékoztatóban ismertetett adatkezelés kapcsán az érintett csak akkor élhet a törléshez való jogával, ha a Belügyminisztériumnak a ráruházott közhatalmi jogosítványok gyakorlása keretében végzett tevékenységének ellátásához, vagy a Belügyminisztérium közérdekű feladatainak végrehajtásához az adat nem szükséges.

5.2. Az adatkezeléssel kapcsolatos érintetti jogok a regisztráció során

5.2.1. A hozzáféréshez való jog

Az érintett jogosult arra, hogy az 1. pontban megadott elérhetőségeken keresztül a Belügyminisztériumtól tájékoztatást kérjen arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e, és ha ilyen adatkezelés folyamatban van, jogosult arra, hogy megismerje azt, hogy

- a Belügyminisztérium
  - milyen személyes adatait;
  - milyen jogalapon;
  - milyen adatkezelési cél miatt;
  - mennyi ideig kezeli; továbbá, hogy
- a Belügyminisztérium kinek, mikor, milyen jogszabály alapján, mely személyes adataihoz biztosított hozzáférést vagy kinek továbbította a személyes adatait;
- milyen forrásból származnak a személyes adatai;
- a Belügyminisztérium alkalmaz-e automatizált döntéshozatalt, valamint annak logikáját, ideértve a profilalkotást is.

A 4.2 pontban megadott azonosítókon kívül nem kerül tárolásra, hogy milyen adatok kerültek kiolvasásra a hozzáférés során.

A Belügyminisztérium az adatkezelés tárgyát képező személyes adatok másolatát az érintett erre irányuló kérésére első alkalommal díjmentesen bocsátja a rendelkezésére, ezt követően adminisztratív költségeken alapuló, ésszerű mértékű díjat számíthat fel.

Az adatbiztonsági követelmények teljesülése és az érintett jogainak védelme érdekében a Belügyminisztérium köteles meggyőződni az érintett és a hozzáférési jogával élni kívánó

személy személyazonosságának egyezéséről, ennek érdekében a tájékoztatás, az adatokba történő betekintés, illetve azokról másolat kiadása is az érintett személyének azonosításához kötött.

5.2.2. A helyesbítéshez való jog

Az okmányazonosító, a korlátozott azonosító és a készülék egyedi azonosító adatok tekintetében nem értelmezhető.

5.2.3. Az adatkezelés korlátozásához való jog

Az okmányazonosító, a korlátozott azonosító és a készülék egyedi azonosító adatok tekintetében nem értelmezhető.

5.2.4. A tiltakozáshoz való jog

Az érintett személy az 1. pontban megadott elérhetőségeken keresztül saját helyzetével kapcsolatos okokból bármikor tiltakozhat az adatkezelés ellen, ha álláspontja szerint a Belügyminisztérium a személyes adatát a jelen adatkezelési tájékoztatóban megjelölt céllal összefüggésben nem megfelelően kezelné. Ebben az esetben a Belügyminisztériumnak kell igazolnia, hogy a személyes adat kezelését olyan kényszerítő erejű jogos okok indokolják, amelyek elsőbbséget élveznek az érintett érdekeivel, jogaival és szabadságaival szemben, vagy amelyek jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódnak.

5.2.5. A törléshez való jog

A tájékoztatóban ismertetett adatkezelés kapcsán az érintett csak akkor élhet a törléshez való jogával, ha a Belügyminisztériumnak a ráruházott közhatalmi jogosítványok gyakorlása keretében végzett tevékenységének ellátásához, vagy a Belügyminisztérium közérdekű feladatainak végrehajtásához az adat nem szükséges.

6. Határidő

A Belügyminisztérium az érintett jogai gyakorlására irányuló kérelmét az annak beérkezésétől számított legfeljebb egy hónapon belül teljesíti. A kérelem beérkezésének napja a határidőbe nem számít bele.

A Belügyminisztérium szükség esetén, figyelembe véve a kérelem bonyolultságát és a kérelmek számát, ezt a határidőt további két hónappal meghosszabbíthatja. A határidő meghosszabbításáról a Belügyminisztérium a késedelem okainak megjelölésével a kérelem kézhezvételétől számított egy hónapon belül tájékoztatja az érintettet.

7. Jogorvoslathoz való jog

Bírósági eljárás kezdeményezése

Az Érintett, az Adatkezelő, illetve – az adatfeldolgozó tevékenységi körébe tartozó adatkezelési műveletekkel összefüggésben – az adatfeldolgozó ellen bírósághoz fordulhat, ha megítélése szerint az adatkezelő, illetve az általa megbízott vagy rendelkezése alapján eljáró adatfeldolgozó a személyes adatait a személyes adatok kezelésére vonatkozó, jogszabályban vagy az Európai Unió kötelező jogi aktusában meghatározott előírások megsértésével kezeli.

A per elbírálása a törvényszék hatáskörébe tartozik. A per – az Érintett választása szerint – az Érintett lakóhelye vagy tartózkodási helye szerinti illetékes törvényszék előtt is megindítható.

Az Adatkezelő az Érintett adatainak jogellenes kezelésével vagy az adatbiztonság követelményeinek megszegésével okozott kárt megtéríti, ugyanakkor mentesül a felelősség alól, ha a kárt az adatkezelés körén kívül eső elháríthatatlan ok idézte elő. Az Adatkezelő nem téríti meg a kárt annyiban, amennyiben az a károsult szándékos vagy súlyosan gondatlan magatartásából származott. Az érintett személyiségi jogának megsértése esetén az érintett sérelmdíjat követelhet.

Hatósági eljárás kezdeményezése

Az Érintett a Nemzeti Adatvédelmi és Információszabadság Hatóságnál (1055. Budapest Falk Miksa utca 9-11, honlap: http://naih.hu; postacím: 1396 Budapest, Pf.: 9.; telefon: +36-1-391-1400; fax: +36-1-391-1410; e mail: ugyfelszolgalat@naih.hu) jogainak érvényesítése érdekében vizsgálatot, illetve hatósági eljárás lefolytatását kezdeményezhet arra hivatkozással, hogy a személyes adatai kezelésével kapcsolatban jogsérelem következett be, vagy annak közvetlen veszélye fennáll, így különösen,

- ha véleménye szerint az Adatkezelő a 7.1.1. pontban meghatározott Érintetti jogainak érvényesítését korlátozza vagy ezen jogainak érvényesítésére irányuló kérelmét elutasítja (vizsgálat kezdeményezése), valamint
- ha megítélése szerint személyes adatainak kezelése során az Adatkezelő, illetve az általa megbízott vagy rendelkezése alapján eljáró adatfeldolgozó megsérti a személyes adatok kezelésére vonatkozó, jogszabályban vagy az Európai Unió kötelező jogi aktusában meghatározott előírásokat (hatósági eljárás lefolytatásának kérelmezése).

Privacy notice

eSzemélyiM (eID card) mobile application

1. Name of the data controller

Ministry of Interior

Registered seat: H-1051 Budapest, József Attila utca 2-4.
Mailing address: H-1530 Budapest, P.O. Box 5
Telephone: + 36 1 441-1000
Fax: + 36 1 441-1437
E-mail address: ugyfelszolgalat@bm.gov.hu

2. Name of the data processor

IdomSoft Informatikai Zrt.

Registered seat: H-1138 Budapest, Váci út 133.

3. Name and contact details of the data protection officer

The data protection officer of the Ministry of Interior: dr. Dominika Tarczi-Ábrahám
E-mail address: adatvedelem@bm.gov.hu

4. Purpose and the legal basis of the data processing

The eSzemélyiM (eID card) mobile application is a card management application which provides the reading of the personal data stored on the eID card for the users (card holders), and which supports the management of the card's PIN and PUK codes.

By using the application, the data detailed below are displayed on the device used for the reading. The application can provide the connection between the mobile device and the card to read the data stored.

The user agreement of the application, as well as the information on registration can be found on the eszemelyi.hu website.

4.1 Processing of the data stored in the chip of the eID card

According to Section 48 of Government Decree No. 414/2015 (XII.23.) on the issue of ID cards and on the uniform image and signature recording rules, a citizen **may verify the contents of the storage element** at the district offices, the designated government office or the body managing the register, personally or **via electronic means following electronic identification.**

In consideration of the above, the data subject may choose to verify the data stored in his/her eID card via electronic means, following electronic identification.

Purpose of the data processing	Reading and display the data on the storage element of the eID card.
Legal basis of the data processing	The data processing is based on GDPR Article 6 (1) e), as well as Section 48 of Government Decree No. 414/2015 (XII.23.) on the issue of ID cards and on the uniform image and signature recording rules.
Data subject	Person authorised to read his/her own data from the storage element of his/her eID card.
Scope of processed data/storage data	– document number – expiry date and issue date – birth name – date of birth – place of birth – gender – family name and given name borne – mother's birth name – personal identification number – TAJ (social security) number – tax identification number – address – place of residence – address abroad – telephone number to be notified in case of emergency – citizenship
Duration of the data processing	Until display on the interface

In order to run the application faster and to use it more conveniently, the application is able to store the CAN number, which is code number required to initiate the protocol for lawful access to the data recorded in the storage element.

The CAN number is stored under the following conditions:

- the CAN number currently entered is stored for 30 minutes, if the application is used continuously,
- when the application is closed, the CAN number will be deleted,
- if the application detects a card with another CAN number, then the CAN number will also be deleted.

4.2 The data processed during the registration

The application **reads personal data from the card,** but only the **document identification number** of the registered person is stored in the background system, which allows the registered person to be identified. In addition to the document identification number, the application also stores the **restricted identifier** (RID) of the card, as well as the **unique identifier** of the device, which are considered anonym data.

Personal data recorded in the card storage element are processed using the e-Identification function. In order to use this function, the user shall have an e-Identification PIN, which has to be activated when the card is first used. Registration may take place after that. **Registration ensures** that the user pairs his/her own eID card with the mobile device. Through the matching, the user may read the data from his/her own card for any number of times, however, the user may do so with other card(s) not matched with the mobile device only for a total of 10 times. **Following the consent** of the eID card holder (entering the e-Identification PIN), during the reading process, the application requests the data access authorisation and the data access needs of the user from the eID server. By using the e-Identification PIN, the application establishes the encrypted radio channel with the card and sends the list of operations approved by the server to the card. The card rememberes this until the time of the transaction. If the channel is established successfully, the application acts as an 'intermediator' between the eID server and the card. The server identifies itself to the card on behalf of the application.

After successful identification, the eID server checks the validity status of the document, as well as the correctness of the data included therein. Afterwards, based on the request the eID server carries out the authorised reading operations, **The card authorises the execution of operations to which the application is entitled and to which the user had given his/her consent.** (If regarding the address data stored in the chip the eID server finds any discrepancy compared to the data stored in the address records, then it shall notify the application, which displays the following message: *'The address/place of residence/foreign address stored in the chip does not correspond to that stored in the personal data and address records.')*

The eID server signals the successful completion of the operation to the application and provides the part of the encrypted response that had been requested by the user in this way. The application displays the response received to the user on the interface.

Purpose of the data processing	Identification of the document registered by the data subject in order to read the data on the storage element of the eID card
Legal basis of the data processing	The data processing is based on GDPR Article 6 (1) e) (the data processing is necessary for the performance of a task performed in the exercise of public authority conferred on the controller)
Data subject	holder of the eID card
Scope of the data processed	– document number – restricted identifier (RID)

	– the unique identifier of the device
Duration of the data processing	The validity period of the document

5. The data subject's rights related to the data processing

5.1. The data subject's rights related to the data stored in the chip of the eID card

5.1.2. Right to access

In accordance with Section 63 of the Preamble of the GDPR, the Data Controller may provide remote access to a secure system which would provide the data subject with direct access to his or her personal data. That right should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software.

5.1.3. Right to rectification

If in course of the reading of the data stored the data subject notices that the data of the telephone number to be notified in case of emergency is not accurate, then the data subject may change these data via electronic means, on the magyarorszag.hu website, following identification. In case of the inaccuracy of other data of the data subject may request the rectification of his/her data in accordance with Section 3 of Government Decree No. 414/2015 (XII.23.) on the issuance of ID cards and on the uniform image and signature recording rules, while proceeding in person, provided that the data subject is able to verify the accuracy of the rectified data in a credible manner.

5.1.4. Right to restriction of data processing

Through the contact details used for proceeding and person and provided in Section 5.1.3 the data subject may request that the processing of his/her personal data be restricted by the Ministry of Interior (with the unambiguous indication of the restricted nature of the data processing and by ensuring processing separate from other data), provided that

- the accuracy of the personal data is contested by the data subject (in this case the Ministry of Interior will restrict the data processing for a period enabling it to verify the accuracy of the personal data);
- the processing is unlawful and the data subject opposes the delete of the personal data and requests the restriction of their use instead;
- the data controller no longer needs the personal data for the purposes of the data processing, but they are required by the data subject for the establishment, exercise or defence of legal claims; or
- the data subject has objected to the data processing (in this case restriction applies to the period until it is verified whether the legitimate grounds of the data controller override those of the data subject).

The data subject may exercise this right directly as well if he/she does not grant access (PIN) to the disclosure of his/her data.

5.1.5. Right to object

Through the contact details provided in Section 1, the data subject may object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him/her, if in the opinion of the data subject, the Ministry of Interior processes his/her personal inappropriately in connection with the purpose specified in the present privacy notice. In this case the Ministry of Interior shall verify that it has compelling legitimate grounds for processing the personal data, which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

5.1.6. Right to delete

In connection with the data processing described in the notice the data subject may exercise the right to delete only if the Ministry of Interior does not need the data for the performance of its activity in the framework of the official authority vested in the Ministry of Interior or the exercise of the tasks of public interest of the Ministry of Interior.

5.2. The data subject's rights related to the data processing during the registration

5.2.1. Right to access

Through the contact details provided in Section 1 the data subject may request information from the Ministry of Interior as to whether or not personal data concerning him/her are being processed, and, where such data processing in progress, then the data subject shall be entitled to the following information:

- data processing by the Ministry of Interior:
  - the personal data concerned;
  - the legal basis;
  - the data processing purpose;
  - the duration of the data processing; as well as
- to whom, when and based on which law have the personal data been disclosed by the Ministry of interior, which personal data are concerned, or to whom the data subject's personal data have been forwarded;
- the source of the personal data;
- whether the Ministry of Interior uses automated decision-making, as well as the logic of such automated decision-making, including profiling as well.

Apart from the identifiers provided in Section 4.2, the data read in course of the access will not be stored.

Upon the request of the data subject, the Ministry of Interior shall provide the data subject with the copy of the personal data subject to the data processing; such data provision shall be free of

charge for the first time, after which the Ministry of Interior may charge a reasonable fee based on the administrative costs.

In order to fulfil the data security requirement and to protect the rights of the data subject, the Ministry of Interior shall ascertain the conformity of the identity of the data subject and the person who wishes to exercise the right to access, to this end the provision of information, the provision of access to the data and the release of any copy of the data are all subject to the identification of the persons concerned.

5.2.2. Right to rectification

Not applicable in respect of the document identifier, the relative identifier and the device unique identifier data.

5.2.3. Right to restriction of data processing

Not applicable in respect of the document identifier, the relative identifier and the device unique identifier data.

5.2.4. Right to object

Through the contact details provided in Section 1, the data subject may object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him/her, if in the opinion of the data subject, the Ministry of Interior processes his/her personal inappropriately in connection with the purpose specified in the present privacy notice. In this case the Ministry of Interior shall verify that it has compelling legitimate grounds for processing the personal data, which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

5.2.5. Right to delete

In connection with the data processing described in the notice the data subject may exercise the right to delete only if the Ministry of Interior does not need the data for the performance of its activity in the framework of the official authority vested in the Ministry of Interior or the exercise of the tasks of public interest of the Ministry of Interior.

6. Time limit

The Ministry of Interior shall fulfil the data subject's request to exercise his/her rights as data subject within one month of the receipt of the request at the latest. The day on which the request is received shall not be calculated in the time limit.

If necessary, and considering the complexity of the request and the number of requests, the Ministry of Interior may extend this time limit by an additional two months. The Ministry of

Interior shall notify the data subject of the extension of the time limit – including the reasons for the delay – within one month of the receipt of the request.

7. Right to legal remedy

Initiation of court proceedings

The Data Subject, the Data Controller or, in the context of processing operations falling within the scope of the processor's activities, the Data Subject may bring the data processor to the court if he considers that the controller or the processor acting on his behalf or acting on the basis of his or her order handles his or her personal data in breach of the requirements laid down in law or in the binding legal act of the European Union.

The court has jurisdiction to adjudicate on the case. At the choice of the Data Subject, the action may also be brought before the competent court of the place of residence or residence of the Data Subject.

The Data Controller shall compensate for any damage caused by the unlawful handling of the Data Subject's data or by breach of the requirements of data security, but shall be exempt from liability if the damage is caused by an unavoidable cause outside the scope of data management. The Data Controller shall not compensate the damage in so far as it results from the intentional or grossly negligent conduct of the injured party. In the event of a violation of the data subject's right to personality, the data subject may claim damages.

Initiation of an administrative procedure

The Data Subject at the National Authority for Data Protection and Freedom of Information (address: 1055 Budapest, Falk Miksa utca 9-11, website: http://naih.hu; postal address: 1396 Budapest, Pf.: 9; telephone: + 36-1-391-1400; fax: + 36-1-391-1410; E-mail: mailto:ugyfelszolgalat@naih.hu) in order to enforce your rights, you may initiate an investigation or an administrative procedure on the grounds that there has been or is an imminent threat of violation of rights in connection with the processing of your personal data, in particular,

- If, in the opinion of the Data Controller, the Data Controller restricts the enforcement of the Data Subject's rights set out in point 7.1.1 or rejects his/her request for the enforcement of these rights (initiation of an investigation), and
- If you consider that, in the course of the processing of your personal data, the Data Controller or the Data Processor acting on its behalf or acting on the basis of its instructions violates the requirements laid down by law or in a binding legal act of the European Union (request for the conduct of an administrative procedure).