

**Belső adatvédelmi szabályzat  
Honda Hungary Kft.**

**Tartalom**

1.	A szabályzat célja és hatálya	1
2.	Az adatvédelem alapfogalmai és elvei	1
	A személyes adat	1
	Az adatkezelés és az adatfeldolgozás	1
	Az adatkezelés célhoz kötöttsége és arányossága	1
	Az adatkezelések szabályai	1
3.	Adatvédelmi nyilvántartás	1
	HHG-n belüli adattovábbítás, adatkezelések összekapcsolása	1
	Adattovábbítás megkeresés alapján	1
	Külföldre irányuló adattovábbítás	1
	Személyes adatok nyilvánosságra hozatala	1
4.	Adatbiztonsági rendszabályok	1
	Számítógépen tárolt adatok	1
	Manuális kezelésű adatok	1
	Az érintett jogai és érvényesítésük	1
5.	Ellenőrzés	1
	Adatvédelmi felelős	1
	Feladatai	1

**Internal Data Protection Regulation  
Honda Hungary Ltd.**

**Contents**

1.	Goals and Objectives of the Regulation	1
2.	Basic Concepts and Principles of Data Protection	1
	Personal data	1
	Data handling and data processing	1
	Purposefulness and proportionality of data handling	1
	Rules of data handling	1
3.	Data Protection Register	1
	Combining data transmission and data handling activities within HHG	1
	Data disclosure upon request	1
	Data disclosure abroad	1
	Dissemination of personal data	1
4.	Data Security Regulations	1
	Data stored on computers	1
	Data handled manually	1
	Rights of the data subjects and their application	1
5.	Verification	1
	Data protection responsible	1
	Tasks:	1

## 1. A szabályzat célja és hatálya

a) E szabályzat célja, hogy meghatározza a Honda Hungary Kft-nél (továbbiakban: HHG) vezetett nyilvántartások működésének törvényes rendjét, valamint biztosítsa az adatvédelem alkotmányos elveinek, az adatbiztonság követelményeinek érvényesülését, s megakadályozza a jogosulatlan hozzáférést, az adatok megváltoztatását és jogosulatlan nyilvánosságra hozatalát.

b) A szabályzat hatálya kiterjed a HHG minden egyes szervezeti egységénél folytatott valamennyi személyes adatokat tartalmazó adatkezelésre.

## 2. Az adatvédelem alapfogalmai és elvei

A személyes adat

**Adatvédelmi tv. 2. § (1)** *E törvény alkalmazása során személyes adat: a meghatározott természetes személlyel (továbbiakban: érintett) kapcsolatba hozható adat, az adatból levonható, az érintettre vonatkozó következtetés.*

a) Személyes adatok az azonosító és a leíró adatok

b) Az érintett egyediesítésére természetes vagy mesterséges azonosító adatok szolgálnak. Természetes azonosító adat különösen az érintett neve, anyja neve, születési helye és ideje, lakóhelyének illetve tartózkodási helyének címe. Mesterséges azonosító adatok a matematikai vagy más algoritmus szerint generált adatok, így különösen a személyi azonosító kód, a társadalombiztosítási azonosító jel (TAJ), az adóazonosító jel, a személyi igazolvány száma, az útlevél száma.

c) A leíró adatok az adatkezelés célja tekintetében releváns egyéb adatok. A meghatározott természetes személlyel kapcsolatba nem hozható leíró adat nem személyes adat (pl. statisztikai adat).

## 1. Goals and Objectives of the Regulation

a) The goal of the present regulation is to determine the lawful processing of registries held by Honda Hungary Ltd. (hereafter referred to as "HHG") and ensure that the constitutional principles of data protection and further data security requirements are met, to prevent unauthorized access and alteration and unauthorized publication of data.

b) The present regulation includes all data management activities concerning personal data at every department within HHG.

## 2. Basic Concepts and Principles of Data Protection

Personal data

**Data Protection Law, Section 2 (1)** *For the application of the law personal data are considered the data that can be linked to a certain natural person (hereafter referred to as "data subject") and a conclusion can be drawn concerning the data subject based on the data.*

a) Personal data are considered identification and descriptive data

b) Natural or artificial data are used to identify the data subject. Natural identification data are considered the name, mother's name, date and place of birth, permanent or temporary home address of the data subject. Artificial identification data are data generated by mathematical or other algorithms, especially the personal identification number, social security number, fiscal identification code, personal ID document number and passport number.

c) Descriptive data are considered other relevant data from the point of view of data management. Personal data that can not be linked to the respective natural person are not considered personal data (for ex.: statistical data).

**Adatvédelmi tv. 2. § (2) különleges adat:**

- a) a faji eredetre, a nemzeti, nemzetiségi és etnikai hovatartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más meggyőződésre  
b) az egészségi állapotra, a kóros szenvedélyre, a szexuális életre, valamint a büntetett előéletre vonatkozó személyes adatok;

Az adatkezelés és az adatfeldolgozás

**Adatvédelmi tv: 2. § (4) a. adatkezelés:** az alkalmazott eljárástól függetlenül a személyes adatok gyűjtése, felvétele és tárolása, feldolgozása, hasznosítása (ideértve a továbbítást és nyilvánosságra hozatalt) és törlése.

a) **Adatkezelő:** a törvény 2. § (4) bekezdés a. pontjában meghatározott tevékenységet végző vagy mással végezhető szervezeti egység.

b) **Adatfeldolgozó:** az adatkezelő megbízásából az utasításai szerint az a) pontban meghatározott tevékenységet végző szervezeti egység.

Az adatkezelés célhoz kötöttsége és arányossága

**Adatvédelmi tv 5. § (1) Személyes adatot kezelni csak meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében lehet.**

a) Személyes adat csak meghatározott törvényes célból, jog gyakorlása és kötelezettség teljesítése érdekében kezelhető, a cél eléréséhez szükséges minimális mértékben és ideig. Ha az adatkezelés célja megszűnt, vagy az adatok kezelése egyébként jogellenes, az adatokat törölni kell.

b) A törlés az adatok felismerhetetlenné tétele oly módon, hogy helyreállításuk már nem lehetséges. Az adatkezelés törlésével, megszüntetésével kapcsolatos tényeket jegyzőkönyvbe kell venni.

**Data Protection Law, Section 2 (2) special data:**

a) personal data concerning race, national identity or nationality, ethnic identity, opinion or party membership, religion or other belief;

b) Personal data concerning the health condition, harmful addiction, sexual life and criminal record of the data subject.

Data handling and data processing

**Data Protection Law, Section 2 (4) data handling:** obtaining, recording and storage, processing and using irrespective of the method applied (including the disclosure and dissemination) and erasure of personal data.

a) **Data controller:** the organization performing by it or by others the activities specified in Section 2 (4) of the respective law.

b) **Data processor:** the organization performing the activities defined under a) on behalf of and according to the directions of the data controller.

Purposefulness and proportionality of data handling

**Data Protection Law, Section 5 (1) Personal data may be handled only having a predefined purpose in order to exercise a right or perform an obligation.**

a) Personal data may be handled only with a predefined lawful purpose to exercise a right or perform an obligation to the minimum extent and time necessary to accomplish the goal. If the purpose of the data handling activity ceases, or the data collection is illegal for certain reasons, the data shall be erased.

b) Erasure is the activity as a result of which the data become unrecognizable and unrecoverable. The facts connected to the erasure of data and cessation of data handling activity shall be registered in a protocol.

### Az adatkezelések szabályai

a) Személyes adat a HHG-n belül akkor kezelhető, ha:

- ahhoz az érintett írásban hozzájárult, vagy
- azt törvény illetve törvény felhatalmazása alapján (Pl.: visszahívási kampány megkeresések) HHG egyéb szabályzatban elrendeli.

b) Az érintettel az adat felvétele előtt közölni kell az adatkezelés célját, valamint azt, hogy az adatszolgáltatás önkéntes vagy kötelező. Kötelező adatszolgáltatás esetén meg kell jelölni az adatkezelést elrendelő jogszabályt.

c) A HHG egyes szervezeti egységeinél adatkezelést végző alkalmazottak kötelesek az általuk megismert személyes adatokat szolgálati titokként megőrizni. Ilyen munkakörben csak az foglalkoztatható, aki **titoktartási nyilatkozatot** tett.

### 3. Adatvédelmi nyilvántartás

**Adatvédelmi tv. 28. § (1)** *Az adatkezelő köteles e tevékenysége megkezdése előtt az adatvédelmi biztosnak nyilvántartásba vétel végett bejelenteni:*

az adatkezelés célját;  
az adatok fajtáját és kezelésük jogalapját;  
az érintettek körét;  
az adatok forrását;  
a továbbított adatok fajtáját, címzettjét és a továbbítás jogalapját;  
az egyes adatfajták törlési határidejét  
az adatkezelő, valamint az adatfeldolgozó nevét és címét (székhelyét), a tényleges adatkezelés, illetve az adatfeldolgozás helyét és az adatfeldolgozónak az adatkezeléssel összefüggő tevékenységét.

a) A HHG-nél létesített minden adatkezelésről nyilvántartást kell vezetni.

### Rules of data handling

b) Personal data may be handled within HHG only if:

- The data subject has provided his written consent or
- based on an assignment of HHG issued in a different regulation based on the law or a lawful authorization (for ex.: contacting customers for call-backs).

b) Before recording the data, the data subject shall be informed about the purpose of data handling and whether data provisioning is voluntary or mandatory. In case of mandatory data provisioning the respective legal measure shall be specified.

c) The employees performing data handling at the different departments of HHG are bound to keep the professional secrecy of personal data they become aware of. Data handling tasks may be performed only by employees who have made a statement of confidentiality.

### 4. Data Protection Register

**Data Protection Law, Section 28 (1)** *the data controller is bound to inform the data protection responsible before starting the activity for registration the following:*

the goal of the data handling;  
the type of data and the legal basis of data handling;  
the range of data subjects;  
the data sources;  
the type of disclosed data, their recipient and the legal basis of data disclosure;  
the date of erasing the different data types;  
The name and address (place of business) of the data processor, the actual location of the data handling and processing, the activities of the data processor connected to data handling.

a) All data handling activities performed at HHG shall be registered.

b) A nyilvántartás dokumentálja az adatkezeléssel kapcsolatos legfontosabb tényeket és körülményeket. Ezek különösen:

- az adatkezelés megnevezése,
- célja, rendeltetése,
- jogszabályi alapja (törvény)
- kezelője (szervezeti egység, annak vezetője, illetve az adatfeldolgozást végző felelős személy neve, beosztása, irodája és telefonszáma),
- érintettek köre és száma,
- nyilvántartott adatok köre,
- adat forrása (maga az érintett, vagy más adatkezelés),
- adattovábbítás (Mely szerv részére? Milyen rendszerességgel?)
- adatbiztonsági intézkedések,
- adatok megőrzésének illetve törlésének ideje.

c) Az adatkezelés megszűnése után a nyilvántartást irattárba kell helyezni és 10 évi megőrzés után selejtezni kell.

HHG-n belüli adattovábbítás, adatkezelések összekapcsolása

**Adatvédelmi tv. 8. § (1)** *Az adatok akkor továbbíthatók, valamint a különböző adatkezelések akkor kapcsolhatók össze, ha az érintett ahhoz hozzájárult, vagy törvény azt megengedi, és ha az adatkezelés feltételei minden egyes személyes adatra nézve teljesülnek.*

a) A HHG szervezeti rendszerén belül a munkavállalók személyes adatai a feladat elvégzéséhez szükséges mértékben és ideig - csak olyan szervezeti egységhez továbbíthatók, amely a munkavállalói jogviszonnyal kapcsolatos adminisztratív és szervezési feladatokat lát el.

b) A HHG-n belüli adattovábbítással kapcsolatos konkrét kérdéseket minden adatkezelés esetében külön kell megállapítani, és az adatkezelés nyilvántartásában rögzíteni.

c) A HHG-nél folyó különböző célra irányuló adatkezelések csak törvényes cél érdekében, indokolt esetben, ideiglenesen kapcsolhatók össze.

b) The registry shall contain all the important facts and circumstances of the data handling. These include especially the following:

- Name of the data handling activity;
- Purpose, destination;
- Legal basis (law);
- Data controller (institutional unit, its manager, the name of the person responsible for data handling, his position, office and telephone number);
- Range and number of data subjects;
- Range of registered data;
- Data source (the data subject or other data handling activity);
- Data disclosure (To which body? At what frequency?);
- Data protection measures;
- Duration of data storage and date of erasure.

c) The registry shall be deposited in the archives after the data handling activities are terminated and eliminated after being preserved for 10 years.

Combining data transmission and data handling activities within HHG

**Data protection law, Section 8 (1)** *The data may be transmitted and the different data handling activities may be combined if the data subject has granted consent or it is permitted by law, and the conditions of data handling are met for each particular type of personal data.*

a) The personal data of employees working within the organizational structure of HHG may be disclosed only to those departments and only to the extent and time necessary, which perform administrative and organizational tasks connected to the employment legal relationship.

b) Actual questions connected to data disclosure within HHG shall be dealt with on a case by case basis and shall be registered in the data handling register.

c) Data handling activities performed at HHG may be combined only for a lawful purpose in justified cases and only temporarily.

d) Az adatkezelések összekapcsolásával kapcsolatos alábbi tényeket jegyzőkönyvbe kell venni:

- az összekapcsolt adatkezelések megnevezése,
- az összekapcsolás célja, rendeltetése,
- az összekapcsolás időpontja és tartama,
- jogszabályi alapja (törvény, belső szabályzat)
- az összekapcsolást végző személy neve, beosztása, szervezeti egysége, irodája és telefonszáma,
- az összekapcsolással érintettek köre és száma,
- az összekapcsolt adatok köre,
- az összekapcsolás módszere (manuális, számítógépes, vegyes)
- adatbiztonsági intézkedések.

e) A jegyzőkönyv első és második példányát az adatkezelések helyén kell őrizni, harmadik példányát pedig a HHG GA-HR osztály részére kell továbbítani. A jegyzőkönyvet 5 évig kell megőrizni.

#### Adattovábbítás megkeresés alapján

a) A HHG-n kívüli hivatalos szervtől vagy magánszemélytől érkező, adatközlésre irányuló megkeresés csak akkor teljesíthető, ha az érintett erre írásban felhatalmazza HHG-t. Az érintett előzetesen is adhat ilyen tartalmú felhatalmazást, amely szólhat valamely időtartamra és a megkereséssel élő hivatalos szervek meghatározott körére.

b) Az érintett nyilatkozattételétől függetlenül teljesíteni kell a büntető ügyekben eljáró hatóságoktól - rendőrség, bíróság, ügyészség, vám- és pénzügyőrség - valamint a nemzetbiztonsági szolgálatoktól érkező megkereséseket. E szervek megkereséseiről az illetékes adatkezelő - közvetlenül vagy szolgálati felettese útján - köteles tájékoztatni az HHG mindenkor felelős Ügyvezető Igazgatóját. Az adatszolgáltatás csak az Ügyvezető Igazgató jóváhagyásával teljesíthető. A Ügyvezető Igazgató a nemzetbiztonsági szolgálatok adatkérésre irányuló megkeresése ellen nem halasztó hatályú panasszal fordulhat az illetékes miniszterhez.

c) A nemzetbiztonsági szolgálatoktól érkező megkeresésre vonatkozó minden adat - a *nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény 42. §-a szerint* - államtitok, amiről sem más szerv, sem más személy nem tájékoztatható.

d) The following facts connected to the combination of data handling activities shall be registered:

- Name of the combined data handling activities;
- Purpose, destination of the combination;
- Date and duration of the combination;
- Legal basis (law, university regulation);
- Name, position, department, office and telephone number of the person performing the combination;
- Range and number of data subjects affected by the combination;
- Range of the combined data;
- Method of combination (manual, computerized, mixed);
- Data security measures.

e) The first and second copies of the protocol shall be retained; the third copy shall be forwarded to the HHG GA-HR department. The protocol shall be kept for 5 (five) years.

#### Data disclosure upon request

a) A request for data disclosure from an official body or private person different than HG may be fulfilled only if the data subject has provided a written authorization to HHG. The data subject may provide such an authorization in advance for a specific period or concerning a specific range of the requesting official bodies.

b) Irrespective of the statement by the data subject the requests submitted by authorities proceeding in penal cases (police, tribunal, prosecution, and customs police) and from national security services shall be fulfilled. The competent data handling commissioner is bound to inform the actual responsible Chief Executive Officer of HHG directly or through his supervisors concerning the requests submitted by these bodies. Data disclosure may be performed only based on the authorization of the Chief Executive Officer. The Chief Executive Officer may submit a non-suspensory complaint to the competent minister against the request for data submitted by the national security services.

c) All data concerning the request submitted by the national security services is a state secret according to Law 75/1995 Section 42 concerning the national security services, and no other official body or person may be informed about this request.

d) A megkeresés alapján teljesített adatszolgáltatással kapcsolatos tényeket, körülményeket jegyzőkönyv felvételével dokumentálni kell. A jegyzőkönyv az alábbi adatokat tartalmazza:

- a megkeresést kezdeményező szerv, vagy személy megnevezése, postacíme, telefonszáma,
- az adatkérés célja, rendeltetése,
- az adatkérés jogszabályi alapja, illetve az érintett nyilatkozata,
- az adatkérés időpontja,
- az adatszolgáltatás alapjául szolgáló adatkezelés megnevezése,
- az adatszolgáltatást teljesítő szervezeti egység megnevezése,
- az érintettek köre,
- a kért adatok köre,
- az adattovábbítás módja.

e) A megkeresésről szóló jegyzőkönyv első példányát az adatkezelés helyén kell őrizni, második példányát pedig HHG GA-HR osztály részére kell továbbítani. A jegyzőkönyvet 5 évig kell megőrizni.

#### Külföldre irányuló adattovábbítás

a) Olyan adatkezelés esetén, amelynél számolni kell külföldre irányuló adattovábbítással (Pl.: DCSI – Ügyfél-elégedettségi program), az érintettek figyelmét erre a körülményre már az adatok felvétele előtt fel kell hívni. Az érintett írásbeli felhatalmazása nélkül személyes adat külföldre nem továbbítható, kivéve ha a törvény ezt lehetővé teszi.

b) A külföldre irányuló adatszolgáltatással kapcsolatos tényeket, körülményeket jegyzőkönyv felvételével dokumentálni kell. A jegyzőkönyv az alábbi adatokat tartalmazza:

- az adattovábbítás címzettje (megnevezés, postacím, telefonszám),
- az adattovábbítás célja, rendeltetése,
- az adattovábbítás jogszabályi alapja, illetve az érintett nyilatkozata,
- az adattovábbítás időpontja,
- az adatszolgáltatást teljesítő szervezeti egység megnevezése,
- az érintettek köre,
- a továbbított adatok köre,
- az adattovábbítás módja.

d) The facts and circumstances connected to the data disclosure performed based on the request shall be documented in a protocol. The protocol shall contain the following data:

- Name, postal address and telephone number of the official body or person submitting the request;
- Purpose, destination of the request for data;
- Legal basis of the request for data, and declaration of the data subject;
- Date of the request for data;
- Name of the data handling activity which is the basis of the data disclosure;
- Name of the department performing the data disclosure;
- Range of the data subjects;
- Range of the requested data;
- Data disclosure method.

e) The first and second copies of the protocol about the request shall be retained; the third copy shall be forwarded to the HHG GA-HR department. The protocol shall be kept for 5 (five) years.

#### Data disclosure abroad

a) In case of data handling where data disclosure abroad may be performed (for ex.: DCSI – Customer Satisfaction Index), the data subjects shall be notified about this prior to recording the data. No data may be transmitted abroad without the written consent of the data subject except when permitted by law.

b) The facts and circumstances connected to the data disclosure abroad shall be documented in a protocol. The protocol shall contain the following data:

- The recipient of the data disclosure (name, postal address, telephone number);
- Purpose, destination of the data disclosure;
- Legal basis of the data disclosure and declaration by the data subject;
- Date of performance of the data disclosure;
- Name of the department performing the data disclosure;
- Range of the data subjects;
- Range of the disclosed data;
- Data disclosure method.

c) A külföldre irányuló adattovábbításról szóló jegyzőkönyv első példányát az adatkezelés helyén kell őrizni, második példányát pedig HHG GA-HR osztály részére kell továbbítani. A jegyzőkönyvet 5 évig kell megőrizni.

#### Személyes adatok nyilvánosságra hozatala

A HHG-nél kezelt személyes adatok nyilvánosságra hozatala - kivéve, ha törvény rendeli el - tilos. A HHG működését bemutató - személyes adatokon is alapuló - statisztikai adatok házon belüli, megfelelő jogosultsági szintek megléte esetén közölhetők.

#### 1. Adatbiztonsági rendszabályok

**Adatvédelmi tv. 10. § (1)** *Az adatkezelő, illetőleg tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek e törvényt, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.*

**(2)** *Az adatokat - kiemelten az államtitokká és a szolgálati titokká minősített személyes adatot - védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, nyilvánosságra hozás vagy törlés, illetőleg sérülés vagy a megsemmisülés ellen.*

Az adatbiztonság megvalósítása érdekében HHG garantálja, hogy a kezelt adatok hozzáférhetők, hitelességük és hitelesítésük biztosított.

e) The first and second copies of the protocol about the data disclosure abroad shall be retained at the location of data handling; the third copy shall be forwarded to the HHG GA-HR department. The protocol shall be retained for 5 (five) years.

#### Dissemination of personal data

Dissemination of personal data handled at HHG (except when required by law) is prohibited. Statistical data prepared based on personal data presenting the operation of HHG may be disseminated if the required in-house authorization levels are met.

#### 1. Data Security Regulations

**Data Protection Law, Section 10 (1)** *The data controller or the data processor within its domain of activity shall ensure the security of data, he is responsible to take the necessary technical and organizational measures and devise the processing regulations, which are necessary to comply with the present law and other data protection and confidentiality regulations.*

**(2)** *Data (especially personal data that have been classified as state secrets or professional secrets) shall be secured especially against unauthorized access, alteration, dissemination or erasure and against damage and destruction.*

For ensuring data security, HHG guarantees that the handled data are accessible and their authenticity and authentication is ensured.

Az Ügyfelek kezelt személyes adatait HHG megfelelő szervezési és műszaki intézkedésekkel védi a jogosulatlan hozzáférésekkel szemben. Ennek biztosítása érdekében a személyes ügyféladatokat tartalmazó informatikai rendszereket csak megfelelő szintű hozzáférés-jogosultsággal rendelkező személyek használhatják. A hozzáférés-jogosultság magában foglalja azt az elvet is, hogy kizárólag olyan terjedelmű hozzáférést kapnak az informatikai rendszert használók, amely a munka elvégzéséhez elengedhetetlenül szükséges és csak azok a személyek, akiknek az adatok kezelése és feldolgozása munkaköri feladata. Ezen hozzáférés-jogosultságokat és azok szintjeit HHG ciklikusan felülvizsgálja.

Az adatbiztonság megvalósítása érdekében HHG garantálja, hogy illetéktelen személyek fizikailag nem férhetnek hozzá sem a papíralapú, sem pedig az informatikai rendszer egyetlen eleméhez sem.

Az adatbiztonsági rendszabályok érvényesítése érdekében a szükséges intézkedéseket meg kell tenni mind a manuálisan kezelt, mind a számítógépen tárolt és feldolgozott személyes adatok biztonsága érdekében.

#### Számítógépen tárolt adatok

A számítógépen, illetve hálózaton tárolt személyes adatok biztonsága érdekében, különösen az alábbi intézkedéseket kell foganatosítani:

*Tükrözés:* A hálózati kiszolgáló gép (a továbbiakban- szerver) a személyes adatok elvesztésének elkerülésére folyamatos tükrözéssel biztosítható egy tőle fizikailag különböző adathordozón.

*Biztonsági mentés:* A személyes adatokat tartalmazó adatbázisok aktív adataiból rendszeresen - a munkavállalói nyilvántartás esetén hetente, a bér- és munkaügyi nyilvántartás, valamint a személyzeti nyilvántartás anyagából pedig havonta - kell külön adathordozóra biztonsági mentést készíteni. A biztonsági mentést tartalmazó adathordozót tűzbiztos fémkazettában kell őrizni.

The personal data of the Clients are protected by the appropriate organizational and technical measures against unauthorized access by HHG. The information technology systems storing the personal data of clients can be used only by persons with the appropriate access authorization level. The access authorization system is based on the principle that access to the information system is granted to the respective parties only to the extent necessary to perform their tasks and only to the persons, whose job description includes data handling and processing. The access authorization levels are periodically reviewed by HHG.

HHG guarantees to ensure data security that unauthorized persons can not have physical access to paper-based documents and to no devices of the IT system.

For the application of the data security regulations all necessary measures have to be taken to ensure the security of the personal data handled manually or stored and processed by computers.

#### Data stored on computers

To ensure the security of personal data stored on computers and computer networks the following measures have to be taken:

*Mirroring:* The network server (hereafter referred to as "server") has to be continuously mirrored on a physically separate data storage unit to prevent the loss of personal data.

*Backup copy:* A backup copy of the active content of databases containing personal data shall be prepared weekly for of employee registers and monthly in case of wages and human resources registers and the content of the human resources records on a separate data storage unit. The data storage unit storing the backup copy shall be stored in a fire-proof metal box.

*Hozzáférés-védelem:* A folyamatos aktív kezelésben lévő iratokhoz csak az illetékes ügyintézők férhetnek hozzá. A személyzeti valamint a bér- és munkaügyi iratokat lemezzszekrényben kell őrizni.

*Archiválás:* Az e szabályzat különös részében említett adatkezelések iratainak archiválását évente egyszer el kell végezni. Az archivált iratokat a HHG mentési szabályzatának megfelelően kell szétválogatni és irattári kezelésbe venni.

*Hálózati védelem:* A mindenkor rendelkezésre álló számítástechnikai eszközök felhasználásával meg kell akadályozni, hogy adatokat tároló, hálózaton keresztül elérhető szerverekhez illetéktelen személy hozzáférjen.

#### Manuális kezelésű adatok

A manuális kezelésű személyes adatok biztonsága érdekében az alábbi intézkedéseket kell fogatosítani:

*Tűz- és vagyonvédelem:* Az irattári kezelésbe vett iratokat jól zárható, száraz, tűzvédelmi és vagyonvédelmi berendezéssel ellátott helyiségben kell elhelyezni.

*Hozzáférés-védelem:* A folyamatos aktív kezelésben lévő iratokhoz csak az illetékes ügyintézők férhetnek hozzá. A személyzeti valamint a bér- és munkaügyi iratokat lemezzszekrényben kell őrizni.

*Archiválás:* Az e szabályzat különös részében említett adatkezelések iratainak archiválását évente egyszer el kell végezni. Az archivált iratokat a HHG mentési szabályzatának megfelelően kell szétválogatni és irattári kezelésbe venni.

*Access protection:* Data shall be accessible only using a valid personal authorization (at least with username and password). Network resources may be accessed only using a valid username and password. Passwords shall be modified regularly. The system administrator shall specify a different password at least every two weeks, users with administrative tasks shall change their passwords at least every forty days.

*Network protection:* By using the available IT equipment unauthorized access of the servers accessible through the network and storing the data shall be prevented.

#### Data handled manually

For the security of personal data handled manually the following measures shall be taken:

*Fire and property protection:* Documents within the archives shall be deposited in a dry, locked room equipped with fire and property protection systems.

*Access protection:* Documents under active continuous handling shall be accessible only to the authorized personnel. Documents used by the human resources, wages and labour department shall be stored in a plate iron cabinet.

*Archiving:* Archiving of documents containing data mentioned in the special section of the present regulation shall be performed on a yearly basis. The archived documents shall be separated and archived according to the archiving regulations of HHG.

Az érintett jogai és érvényesítésük

**Adatvédelmi tv. 11. § (1) Az érintett**

a) *tájékoztatást kérhet személyes adatai kezeléséről (12. és 13. §), valamint*

b) *kérheti személyes adatainak helyesbítését, illetve - a jogszabályban elrendelt adatkezelések kivételével - törlését (14–16. §).*

a) Az érintett az illetékes ügykezelőtől tájékoztatást kérhet a róla szóló adatkezelésről és abba bele is tekinthet. A betekintést úgy kell biztosítani, hogy ez alatt az érintett más személy adatait ne ismerhesse meg.

b) Az érintett kérelmére az adatkezelő tájékoztatást ad az általa kezelt adatairól, az adatkezelés céljáról, jogalapjáról, időtartamáról, továbbá arról, hogy kik és milyen célból kapták meg az adatokat.

c) A tájékoztatás illetve a betekintés biztosítása csak akkor tagadható meg, ha a kért adatokat az illetékes szerv a megfelelő eljárás keretében - az államtitokról és a szolgálati titokról szóló 1999. évi LXV. törvény szabályai szerint - előzetesen államtitokká vagy szolgálati titokká nyilvánította, az adatkezelő köteles az érintettel a közlés megtagadásának indokát közölni.

d) Adatváltozás vagy téves adatrögzítés észlelése esetén az érintett kérheti kezelt adatainak helyesbítését illetve kijavítását. A téves adatot az adatkezelő két munkanapon belül helyesbíteni köteles.

e) Nem kötelező adatszolgáltatáson alapuló adatkezelés esetén az érintett indoklás nélkül kérheti kezelt adatainak törlését. A törlést két munkanapon belül el kell végezni.

Adatkezeléssel kapcsolatos jogainak megsértése esetén az érintett az illetékes szervezeti egység vezetőjéhez (Osztályvezető, Ügyvezető Igazgató) fordulhat. Az Osztályvezető és az érintett közötti vitában az Ügyvezető Igazgató dönt.

Rights of the data subjects and their application

**Data Protection Law, Section 11 (1) The data subject may**

a) *Request information about handling of his personal data (Section 12 and 13);*

b) *Request the correction of his personal data and their erasure (except for the data handling processes requested by law) (Section 14–16);*

a) The data subject may request information from the administrative personnel about the handling of his personal data and may examine these data. Examination of the data shall be provided in a manner so as the data subject does not see the data of others.

b) The data controller shall provide information about the data handled by him, the purpose, legal basis and duration of the data handling activity upon the request of the data subject and also about who and for what purpose has received the data.

c) Notification and examination may be refused only if the competent authority has already classified the requested data through the appropriate procedure as state or service secret according to Law 65/1999. Concerning state and service secrets; the data controller is bound to inform the data subject about the motivation of the refusal.

d) In case of data modification or when recognizing incorrect data recording, the data subject may request the correction or rectification of the handled data. The data controller is bound to correct the incorrect data within two working days.

e) In case of data handling not based on compulsory data provisioning, the data subject may request the erasure of the handled data without any justification. Erasure shall be performed within two working days.

In case of infringing the rights connected to data handling, the data subject may appeal to the manager of the respective department (head of department, chief executive officer). The Chief Executive Officer shall decide in case of disagreement between the data subject and the Head of Department).

## 5. Ellenőrzés

a) Az adatvédelemmel kapcsolatos előírások, így különösen jelen szabályzat rendelkezéseink betartását, az adatkezelést végző szervezeti egységek vezetői folyamatosan ellenőrzik.

b) A HHG Belső Adatvédelmi Felelőse, valamint a GA-HR osztály vezetője az irat- és adatkezeléssel kapcsolatos szabályzatok, jegyzőkönyvek és a nyilvántartás áttekintésével gondoskodik az adatkezelés törvényes rendjének megtartásáról. Törvénysértés esetén az Ügyvezető ennek megszüntetésére szólítja fel az adatkezelőt.

c) Az adatbiztonsági rendszabályok és intézkedések megtartását az Ügyvezető által kinevezett belső ellenőr és egy informatikus munkatárs ellenőrzi.

d) Az egyes adatkezelések ellenőrzését szükség szerint, de legalább évente egyszer el kell végezni. Az ellenőrzés tapasztalatairól a belső ellenőr, írásban tájékoztatja az Ügyvezetőt.

## 5. Verification

a) Compliance with the regulations connected to data security especially with the dispositions of the present regulation shall be continuously verified by the managers of the departments performing data handling.

b) The Internal Data Protection Commissioner of the HHR and the manager of the GA-HR department shall ensure compliance with the regulations concerning data handling by reviewing the regulations connected to documents and data handling, protocols and registers. In case of violating the law the Executive Officer shall summon the data controller to discontinue the respective activity.

c) The internal commissioner and IT technician appointed by the Chief Executive Officer shall control compliance with the data protection regulations and measures.

d) Verification of the different data handling activities shall be performed as necessary but at least once a year. The internal commissioner shall inform the Chief Executive Officer about the results of the inspection.

## Adatvédelmi felelős

A HHG belső adatvédelmi felelőse: Szabó Zoltán

Levélcím: 2040 Budaörs, Törökbálinti u. 25/b.

Tel: (23) 506 409

E-mail: [zoltan.szabo@honda-eu.com](mailto:zoltan.szabo@honda-eu.com)

### Feladatai

- Az adatkezelés feltételeinek felülvizsgálata
- Az érintetteknek nyújtott tájékoztatás rendszerének felülvizsgálata
- A belső adatvédelmi szabályzat felülvizsgálata
- Az érintettek jogai érvényesülésének felülvizsgálata
- Az adatvédelmi biztossal kapcsolatos tennivalók.

Jelen Adatvédelmi Szabályzat mindenkor aktuális példánya megtalálható a [www.honda.hu](http://www.honda.hu) weboldalon.

Budaörs,

2008.08.01

.....

Ügyvezető/Managing Director

## Data protection responsible

Internal data protection responsible of HHG:  
Szabó Zoltán

Postal address: 2040 Budaörs, Törökbálinti u.  
25/b.

Tel: (23) 506 409

E-mail: [zoltan.szabo@honda-eu.com](mailto:zoltan.szabo@honda-eu.com)

### Tasks:

- Inspection of data handling conditions;
- Inspection of the information system provided to the data subjects;
- Inspection of the internal data protection regulation;
- Inspection of granting the rights to data subjects;
- Tasks connected to data protection responsible.

The current copy of the present Data Protection Regulation is available at [www.honda.hu](http://www.honda.hu).

