A.P.P. Trading and Service Provider Ltd.
9028 Győr, Fehérvári Street 75.

DATA PROTECTION AND DATA MANAGEMENT REGULATIONS

Scope of competence: Management	**Approval(s) signature:**			**Applicable: Since 25.05.2018**
Responsible/person in charge: BR (right)	**Accepted:** 23.05.2018	**Announced:** 24.05.2018	**Way of announcement:** received on office@diadem.com e-mail address	
The document of "pdf" extension is the valid!	**Document name:** Adatvedelmi_es_Adatkezelesi Szabalyzat_Public			**Version number:** 2018_01

1. The purpose of the Regulations

A.P.P. Trading and Service Provider Ltd. (hereinafter referred to as: Data Manager) by this Regulations,

- applicable since 25 May 2018,
- in order to comply with the European Parliament and Council's (EU) no. 2016/679. Regulation (hereinafter referred to as the GDPR), and
- the relevant Hungarian legislation, in particular with regards to Act CXII of 2011 on Information self-determination right and the freedom of information (hereinafter: Infolaw)

adopts the following data management regulations by the undersigned place and time.
The purpose of this Regulations is to record the data protection and data management principles and rules applied by the Data Manager, and the Data Manager's data protection and data management policy.
The Regulations, in addition to the Data Manager, applies to its organizations who have a place of business in the European Economic Area (EEA) or who handle the personal data of natural persons in the EEA.
This Regulations is binding to all employees of the Data Managers and to persons who are in a commissions legal relationship with it.

2. Data of the Data Manager

Name:	[**A.P.P. Trading and Service Providing Ltd.**]
Registered office (mailing address):	[**9028 Győr, Fehérvári Street 75.**]
Company Registration Number:	[**08-09-007336**]
Tax Number:	[**11611989-2-08**]
Data protection registration number:	[Not relevant[1]]
Telephone contact:	[+36 96 / 512 910]
Electronic contact:	[info@diadem.com]
Legal representatives:	Péter Csizmadia, Szilárd Csizmadia, Renáta Berkes, Alexandra Sinkó

3. Data protection legislation

Legislation of major importance regarding the Regulations:

The European Parliament and the Council's (EU) Regulation no. 2016/679 (hereinafter referred to as "GDPE Regulation")
Basic Law of Hungary
Act CXII of 2011 on Information self-determination right and the freedom of information (hereinafter: Infolaw)
Act V of 2013 on The Civil Code 2013. act (hereinafter referred to as: Civil Code.)
Ac I of 2012 on the Labour Code (hereinafter referred to as: LC.)

[1] The Data Manager employs less than 250 people and does not fall under the exceptions of enterprises employing fewer than 250 persons, based on which it would have a register managing obligation, and therefore recording it into data protection register is not justified.

4. Concept explanation

All the definitions in this section are defined in Article 4 of the GDPR as follows:
***Data Processor*:** is a natural or legal person, a public authority, agency or any other body that manages personal data on behalf of the data manager;
***Place of business of the Data Processor*:** if a data processor having its places of business in more than one Member State, this is its central place of administration in the Union or, if the data processor does not have a central place of administration in the Union, then the place of business of the data processor within the Union where the main data management activities are performed, if the data processor is subject to obligations under this Regulation;
***Data management*:** any operation or the sum of operations performed in automated or non-automated way on personal data or data files, by means of collection, recording, organization, division, storage, transformation or alteration, retrieval, access, use, transmission, distribution, dissemination or making available in any other way, harmonization or interconnection, restriction, deletion or destruction;
***Data Manager*:** any natural or legal person, public authority, agency or any other body that determines the purposes and means of managing personal data individually or with others; if the purposes and means of data management are defined by Union or national law, the Data Manager or the particular aspects of the designation of the Data Manager may also be defined by the Union or national law;
***Place of business of the Data Manager*:** if a data manager has its places of business in more than one Member States, this is its central place of administration in the Union or, if the data manager makes its decisions regarding the purposes and means of personal data management at another place of business within the Union, and the latter place of business has the competence of making these decisions, then the place of business, that makes these decisions, shall be considered as central place of business;
Data protection incident: damage of the security, resulting in accidental or unlawful destruction, loss, alteration, unauthorized disclosure or unauthorized access to transmitted, stored or otherwise managed personal data;
***Anonymisation*:** the management of personal data in a way that, without the use of any additional information, it can no longer be ascertained that which personal data belongs to which specific natural person, provided that such additional information is stored separately and with specific technical and organizational measures it is ensured that the identified or identifiable natural persons cannot be linked to the personal data;
Recipient: a natural or legal person, a public authority, agency or any other body to whom or to which the personal data is communicated, regardless if it is a third party. Public authorities which have access to personal data in an individual investigation in accordance with the Union's or a state member's national law, shall not be considered recipients; the management of such data by these public authorities must comply with the applicable data protection rules in accordance with the purposes of the data management;
Medical data: personal data related to the physical or psychological health of a natural person, including data related to health services provided to a natural person, that carries information on the health of the natural person;
Data subject: the identified or identifiable natural person whose personal data is managed by the Data Manager or the Data Processor;
Contribution of the data subject : a voluntary, specific statement of will of the data subject based on appropriate and explicit information, by which the data subject indicates his/her contribution to the processing of his/her personal data in a statement or by an unambiguous confirmation act;
Third-party: the natural or legal person, public authority, agency or any other body which is not identical with the data subject, the data manager, the data processor or the persons who have authorization for data management under the direct control of the data manager or the data processor;
***Profiling*:** any form of automated processing of personal data, whereby personal data are evaluated for assessment of certain personal characteristics associated with a natural person, in particular analyzation or forecasting of features related to work performance, economic situation, health status, personal preferences, interests, reliability, behaviour, residence or movement;
***Special categories of personal data*:** personal data related to racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, also genetic, biometric and

health data for the unique identification of natural persons, as well as personal data relating to the sexual life or sexual orientation of natural persons.
Personal data: any information relating to an identified or identifiable natural person ("Data subject"); a natural person is identifiable, who can be identified directly or indirectly, specifically based on an identifier, such as name, number, location data, online identifier or on one or more factors relating to the physical, physiological, genetic, intellectual, economic, cultural or social identity of the natural person.

- // -

Governing law of European Union: the GDPR and its revised, superseded and repealed versions, including legislation implementing or supplementing GDPR, and 2002/58/EC Electronic Communications Data Protection Regulation (and its amending Regulation 2009/136), which will be replaced by the Electronic Communications Data Protection Regulation expected to enter into force in 2018;
Supervisory authority**:** an independent public authority of a member state, created in accordance with article 51. In Hungary, this is the role of the National Data Protection and Information Freedom Authority (1125 Budapest, Szilágyi Erzsébet Alle 22/c.; https://www.naih.hu/panaszuegyintezes-rendje.html, hereinafter referred to as NAIH (Nemzeti Adatvédelmi és Információszabadság Hatóság)).

5. The principles of data management

5.1. Legality, fair procedure and transparency

The management of personal data shall be lawfully and fairly done, and in a manner transparent to the Data subject, the consent of the Data subject is necessary for this, as well as his/her consent to manage his/her data.

The Data Manager manages the personal data of the natural person Data subjects by this Regulations, regarding the performance of an agreement based on the written contract and/or real act between the parties, based on the voluntary, informed and definitive consent of the Data subjects, in accordance with the Infolaw 5§ Section 1), and if it is necessary for the fulfilment of a legal obligation, or to enforce a legitimate interest of the data manager or a third party, and by enforcing this interest, restricting the right to protection of personal data, is in compliance with the Infolaw 6§ Section 1).

5.2. Bound to purpose

Collecting personal data can only be done for a specific, clear and legitimate purpose and data cannot be managed in a way that is incompatible with these goals; further data management for the purpose of public interest archiving, for scientific and historical research purposes or for statistical purposes is not considered to be incompatible with the original purpose.

The Data Manager declares that personal data is handled only in order to exercise his/her rights or to fulfil his/her obligations. The managed personal data shall not be used for private purposes, and data management is always in compliance with the principle of bound to purpose - if the purpose of the data management is terminated or the data management is otherwise illegal, the data will be deleted.

5.3. Data frugality

Personal data must be appropriate and relevant for the purposes of data management and should be limited to the need.

5.4. Accuracy

Personal data must be accurate and, if necessary, up-to-date; all reasonable measures must be taken to correct or immediately delete any inaccurate personal data for the purposes of the data management.

Given that each personal data will always be given to the Data Manager on the voluntary, informed and explicit consent of the Data subject, in case of the personal data of those Data subjects, where the personality of the Data subject and the person providing the relevant personal data are not the same, the Data subject is responsible for the actuality and management of the personal data; except if the potential bad faith of the Data Manager would exclude such liability.

5.5. Limited transparency

Personal data must be stored in a form that

- makes the identity of the Data subjects available only for the time necessary to achieve the purposes of personal data management;
- the storage of personal data for a period of time longer than this, may only take place if personal data is processed for purposes of public interest archiving, for scientific and historical research purposes or for statistical purposes,

it takes into account the implementation of the appropriate technical and organizational measures for the protection of the rights and freedoms of the Data subjects affiliated in GDPR.

5.6. Integrity and confidentiality

Personal data should be managed in such a way as by using appropriate technical or organizational measures, the adequate security of personal data, the protection against unauthorized or unlawful management, accidental loss, destruction, or damage to data is ensured.

5.7. Accountability

The Data Manager is responsible for the compliance as per section 5.4, and must be able to demonstrate compliance.

6. Informing Data subjects

6.1. Scope of managed personal data

6.1.1. ID copies

- personal ID
- address card
- Tax card

6.1.2. Other data: employees (in the case of this part, the relevant section of the current Personal Data Handling Regulations is governing, this list is not complete)

- Social security number,
- bank account number,
- number of children, year of birth,
- private pension funds,
- health insurance fund
- phone number
- e-mail address
- employment health compliance data

6.1.3. School certificates

- copies of qualification certificate;
- language exam certificate;
- driving license

6.1.4. Personal characteristics (employees)

6.1.5. Customer stock

- company representative's
  - name
  - e-mail address
  - phone number
- individual's
  - name
  - e-mail address
  - phone number
  - tax number

6.1.6. Supplier staff

- company representative's
  - name
  - e-mail address
  - phone number
- individual's
  - name
  - e-mail address
  - phone number
  - tax number

6.1.7. Service providers, operators

- company representative's
  - name
  - e-mail address
  - phone number
- private person / private entrepreneur
  - name
  - e-mail address
  - phone number
  - tax number
- cooperating partners (engineering firms, IT consultants, legal advisers, translators, etc.)
  - company representative's
    - name
    - e-mail address
    - phone number
  - private person / private entrepreneur
    - name
    - e-mail address
    - phone number
    - tax number

6.1.8. Tenants

- company representative's
  - name
  - e-mail address
  - phone number
- individual's
  - name
  - e-mail address

- phone number
- tax number

6.1.9. Additional data to be protected

- electronic surveillance system
- making photo, audio, video recordings

6.2. Purpose and legal basis for each data processing

The purpose and the legal basis for the managing the personal data listed in Section 5.1. may be as follows:

a) the consent of the Data subject
b) performance of contract
c) compliance with a legal obligation of the Data Manager
d) necessary for the vital interests of the Data subject or another natural person
e) public interest data management or mandatory data provision towards third parties, public authorities
f) necessary for the enforcement of the Data Manager's or a third party's legitimate interests
g) personal and property protection

The management of the personal data recorded in Section 5.1 may have more than one legal basis from those listed above.

5.1.1.	*ID copies*	[a; d; e]
5.1.2.	*Other data (employees)*	[a; d; e]
5.1.3.	*School certificates*	[a; d; e]
5.1.4.	*Personal characteristics (employees)*	[a; d]
5.1.5.	*Customer stock*	[b; c; d; e]
5.1.6.	*Supplier stock*	[b; c; d; e]
5.1.7.	*Service providers, operators*	[b; c; d; e; f]
5.1.8.	*Tenants*	[b; d; f]
5.1.9.	*Additional data to be protected*	[a; g]

6.3. Contact details of the Data Protection Officer / person(s) liable for data protection

6.3.1. Data Protection Officer

No data protection officer has been designated at the Data Manager.

Justification:

- The Data Manager is not regarded as a public authority, or other body carrying out public tasks.
- The Data Manager does not have a major activity that requires regular, systematic, large-scale monitoring of the Data subjects.
- Main activities of the Data Manager do not affect special categories of personal data.
- The Data Manager's main activity is not managing HR data.

6.3.2. Person(s) liable for data protection

At the Data Manager, persons in the following areas were appointed liable for data protection:

Department / area	Relevant data	Person	Responsible's name
Sales department	customer database	3	Mária Zierhut Sylvia Nyiri, née Páli

			Szonja Jenei
Acquisition department	supplier database	1	Henriett Tendl
Technical department	service provider, contributor database	1	Anikó Tarjáni
Finance department	corporate accounting, controlling, payroll	1	Alexandra Sinkó
Marketing department	publications, sound and visual appearance, customer invocation (online and traditional), website management	1	Benjamin Köpeczi-Bócz
HR and legal	recruitment, labour legal relationship, general contracts	1	Renáta Berkes

6.4. Recipients of managed personal data, categories of the recipients

Given the fact that the data manager does not apply any data processor service provider for personal data management, thus no personal data will be transmitted to third parties.

The personal data contained in the customer and supplier database can be managed by the sales and supplier staff of the Data Manager for customer relationship purposes, while the marketing staff can manage it for electronic discounts and advertising purposes, respecting the directives set in the GDPR.

The personal data of the Data Manager's employees can be managed by the Data Manager's HR and Finance staff for the purpose of creating and maintaining the employment relationship, while respecting the directives set in the GDPR.

Audio and visual appearance made by the Data Manager may be processed by the Marketing staff of the Data Manager in compliance with the directives set in the GDPR.

The Data Manager is required to provide personal information to third parties (public authority: statistics office, tax office, etc.) in accordance with the relevant legal provisions.

6.5. The duration of personal data storage

As a general rule, until the data management purpose is achieved.

Until rights and obligations related to legal rights are terminated.

In addition, until the time set out in the relevant legislation(s).

Until the consent of the Data subject has been withdrawn and/or the cause of the consent has been reached, ceased or failed.

In connection with employment rights and obligations, until the termination of employment.

Regarding rights arising out of employment, until the deadline specified in the legislation on the payment of pensions.

Accounting certificates (including G/L accounts, analytical and detailed records), which directly and indirectly support the accounting, must be maintained in a readable form for at least eight years, retrievable as per the reference of the accounting records.

The storage period for the personal data of the customer and supplier database - given that the storage of personal data is not only a lawful obligation and legitimate interest of the Data Manager but also the legitimate interest of the Data subject - is until the Data subject exercises his/her right of opposition. That is, if the Data subject withdraws his/her consent to the storage of his/her personal data, or opposes against the storage of his/her data in any of the two databases, the personal data will be deleted.

6.6. The personal data service

a) is based on legislation
b) is based on contractual obligations
c) is a precondition of a contract

6.7. Provision of personal data

The Data subject shall provide his/her personal data.

The failure of data provision may have the following possible consequences:
- failure of contracting assignment, legal relationship of service and sales relationship
- termination of contracting assignment, legal relationship of service and sales relationship
- failure of fulfillment of contract-based obligations;
- failure of work relationship establishment
- endangering sustainability of work relationship
- suspending work relationship
- failure to fulfill obligation of the Data Manager in regards of work relationship

6.8. Personal data management

The Data Manager does not manage the personal data or any part of the personal data of the Data subject in an automated manner.

If the Data Controller intends to perform data processing for purposes other than the purpose for which they are collected, the Data Manager informs the Data subject about this intention, and obtains his/her prior express consent or gives him/her the opportunity to prohibit the use.

The Data Manager is obliged to correct the personal data that is not real. The personal data will be deleted by the Data Manager if its management is unlawful, if the Data subject requests for it - in this case within a maximum of five (5) days - if it is incomplete or incorrect - and this status cannot be legally corrected -, provided that the deletion is not excluded by legislation, if the purpose of data management has ceased, if the statutory deadline for data storage has expired or it is ordered by the court or by the National Data Protection and Information Authority. The Data Manager informs the Data subject about the correction or deletion, as well as those, to whom the data were previously forwarded for data processing. Notification may be omitted if it does not prejudice the legitimate interest of the Data subject for the purpose of data management.

If the Data subject uses personal data in an Illegal or misleading manner, or the Data subject commits a crime, the Data Manager reserves the right to retain the so-used relevant data as evidence, until the termination of any litigation or non-litigation procedure. The latter shall also apply to the case where the Data subject has requested the deletion of the relevant personal data in order to hinder, but at lease make it difficult for the Data Manager to enforce its legitimate claims.

7. Rights of Data subjects

7.1. Access and other rights

The Data subject may apply to the Data Manager for access, correction, deletion, or limitation of the relevant personal data and may object against the management of such personal data.

The Data subject, during the management of his/her personal data, may apply for the access of the following data:

- purpose of data management
- categories of the personal data of the Data subject
- scope of recipients
- the duration of personal data storage
- if the source of collected personal data is not the Data subject, the source of their acquisition

At the request of the Data subject, a copy of the personal data shall be made available to the Data subject. For additional copies of data requested by the Data subject, the Data Manager may charge a reasonable administrative fee.

The Data subject may object against the data management, in particular if

- the management or transmission of personal data is only necessary to fulfil the legal obligation of the Data Manager, or to enforce the legitimate interests of the Data Manager, data recipient or a third party, except in the case of mandatory data management;
- the purpose of management or transmission of personal data is direct solicitation, polling or scientific research; and
- in other cases specified by law.

The Data Controller shall examine the objection within the shortest possible time, but not later than fifteen (15) days after the submission of the request, makes a decision on its merits and informs the applicant in writing. For the duration of the examination, but for a maximum of five (5) days, the Data Manager will suspend the processing of data. If the objection is justified, the head of the organizational unit managing the data shall act as specified in the applicable law.

If the Data Manager determines the validity of the Data subject's objection, the data management - including further data collection and data transfer - will be terminated, the Data manager will lock the data, and inform all person to whom data have been transmitted and who are obliged to take action to enforce the right to protest about the objection and about the measures taken on the basis of the decision.

If the Data subject does not agree with the decision of the Data Manager or if the Data Manager fails to comply with the deadline, the Data subject may appeal to court from the notification of the decision or within thirty (30) days from the last day of the deadline.

7.2. Right to data portability

The Data subject is entitled to data portability rights. The Data subject's personal data provided by him/her to the Data Manager may be obtained in an articulated, widely used, machine-readable format, and may forward these to another data manager.

The right to data portability may be linked to specific titles, such title is the consent of the Data subject, and the performance of the contract.

7.3. Right to the withdrawal of consent

In the case of consent-based data management, the right to withdraw the consent at any time, which does not affect the lawfulness of the data management performed on the basis of the consent prior to the withdrawal.

7.4. Needs validation, right to complain

The Data subject may exercise his/her rights with appeal to court according to Act V. of 2013 on the Civil Code, and the content of the Infolaw, and may appeal to and make complaint to the NAIH (mailing address: 1534 Budapest, POB.: 834; address: 1125 Budapest, Szilágyi Erzsébet alle 22/c.).

The court will proceed in the case as priority.

8. Data Manager's obligations

8.1. Data security measures

The Data Controller shall make every effort to ensure the security of the data of the Data subjects, shall take the necessary technical and organizational measures and shall develop the procedural rules which are necessary to enforce data- and privacy protection rules, on the one hand, in order to implement the data protection principles, and on the other hand in order to meet the requirements of the GDPR.

When defining certain measures, the Data Manager takes into account the following risks:
the managed personal data's

- accidental or unlawful destruction,
- loss,
- alteration,
- unauthorized disclosure, or

unauthorised access.

The Data Manager performs data management primarily in a paper-based manner, secondary via machine-processing.

Data security measures:

- Continuous legal validation and system upgrading of the SAP corporate management system
- signing confidentiality declarations with employees who manage personal data
- introduction of IT Data Protection Regulations
- Continuous password changing
- introduction of Wifi Data Protection Regulations
- introduction of Camera Data Protection Regulations
- introduction of Use of IT Devices Regulations
- Manage administrator and user permissions, lock the folder system, and define authorizations

Data management is performed by Data Manager itself, the data management site is at the Data Manager's head office: 9028 Győr, Fehérvári Street 75., in a separate server room created for this purpose, with closed servers protected with permission settings.

The data is physically managed at the location described above, and the data of the Data subjects are stored here.

Data that are automatically, technically recorded in the Data Manager's system(s), will be stored in the system from the time they are generated until a reasonable period of time, in order to ensure the system's operation. The Data Manager ensures that these automatically recorded data cannot be linked to other personal data, except in cases that are legally binding. If the Data subject has terminated or objects against his/her consent to the management of his/her personal data, then his/her identity will not be identifiable by the technical details - except for by the investigating authorities and their experts.

If this occurs, the data management personnel at the Data Manager's organizational units are required to keep the personal information they are aware of as business secret. For this purpose, the personnel who manage and have access to the personal data have signed a ***confidentiality statement***. At the same time, the Data Manager's staff, during their work, are also obliged to take care of the prevention of unauthorized person's access to personal data. The storage and placement of personal data is designed to be unavailable, unrecognizable, unalterable or indestructible by an unauthorized person.

The senior officer of the Data Manager with a prevailing decision-making competence defines the data protection organization, defines the data protection- and the related tasks and responsibilities, and selects the person who handles the data management, taking into account the specialties of the Data Manager.

The Data Manager will review and, if necessary, update the measures taken.

8.2. Ensuring data management bound to purpose

The Data Manager ensures that only such personal data is managed, which is necessary for the specific data management purpose. This refers to the amount, the extent of management, the duration of storage and the availability of personal information collected. It must be ensured that personal data cannot become accessible for an undetermined number of people, without human intervention by default.

8.3. Registration obligation

The Data Manager does not keep records of its data management activity, as per GDPR Section 1 Article 30 par. 5), according to which data management activities are not subject to record keeping obligations for enterprises employing less than 250 persons, unless

- the processing of data entails a risk to the rights and freedoms of the Data subject; or if
- it affects special personal data, or if
- it means the management of personal data relating to resolutions and crimes regarding determining criminal liability.

8.4. Obligations for data management incidents

The Data Manager has the following obligations regarding data management incidents:

- the incident must be reported to the NAIH within 72 hours after learning about the incident, unless the data protection incident probably does not pose a risk to the rights and freedoms of natural persons;
- if the notification does not happen within 72 hours, the reasons for proving the delay must also be attached;
- the information in the notification may be communicated in several portions, without causeless delay;
- recording of data protection incidents shall happen with indicating the related facts, and fixing the remedies;
- informing the Data subjects about the data protection incident in the case of conditions occurring as per Article 34 of GDPR, as defined therein.

8.5. Performing data protection impact assessment

The Data Manager, according to Article 35 of the GDPR, *shall perform data protection impact assessment* in the case the planned data management is likely to pose high risk on the rights and freedoms of the Data subjects. The purpose of the assessment is to see how the planned data management operations affect the protection of personal data. In the course of the assessment, the Data Manager asks the opinion of the Data subjects or their representatives on the planned data handling. The Data Manager shall, if necessary, but at least in case of change in risks reported by the data management operations, carry out an assessment to evaluate whether the personal data management is in accordance with the data protection impact assessment.

9. Other provisions

Regarding
- the data management of the Data Manager's website and its relevant services,
- the data management of the Data Manager's employees (Human Resources Data Management Regulations);
- the data management of the Data Manager's monitoring system suitable for picture- and audio recording,
- wifi use of the Data Manager

separate policies apply, if for any reason, more data protection rules might be applicable to the specific data management of the Data Manager, and in this case the provisions of this Regulations shall govern, together with the relevant differences in the additional regulations.

During the execution of the tasks of the Data Manager, it shall cooperate with the NAIH - on the basis of its request.

The Data Manager shall ensure that these Regulations are revised and updated as necessary.

The Data Manager is entitled to modify the content of this Regulations unilaterally; in this case, notification of the Data subjects is required.

Issues not regulated in these Regulations are governed by the provisions of Hungarian law on data protection, in particular the Infolaw, and the provisions of GDPR applicable from 25 May 2018 shall apply.

10. Annexes

1. Annex No. 1: Data deletion protocol
2. Annex No. 2: Data protection incidents register
3. Annex No. 3: Notification letter about information protection incident
4. Annex No. 4: Consent to management of personal data
5. Annex No. 5: Withdrawal of data management consent
6. Annex No. 6: Confidentiality statement

Annex No. 1:

P r o t o c o l

– About the deletion of personal data of ..... Data subject –

Made: In year 2018, ... month.... day, at ..... hours and ..... minutes, at the seat of

APP Ltd.

Company Registration Number:	08-09-007336
Seat:	9028 Győr, Fehérvári Street 75.
Tax Number:	11611989-2-08
Electronic contact:	info@diadem.com
Phone:	96 / 512 910
Legal representatives:	Péter Csizmadia, Szilárd Csizmadia, Renáta Berkes, Alexandra Sinkó

as data manager (hereinafter referred to as "**Data Manager**"); on behalf of the Data Manager ..... **in relation with .....** (additional data necessary for identification[2]**: .....), regarding the deletion of managed, stored personal data (hereinafter referred to as "Data deletion") of the data subject natural person (hereinafter referred to as "Data subject").**

Following persons are present, taking part in Data deletion:

Name:	**……**
Address:	**……**
Authorization and its basis *(reference to relevant internal regulations and/or appropriate sections of legislation)***:**	**……**

Name:	**……**
Address:	**……**
Authorization and its basis *(reference to relevant internal regulations and/or appropriate sections of legislation)***:**	**……**

Name:	**……**
Address:	**……**
Authorization and its basis *(reference to relevant internal regulations and/or appropriate sections of legislation)***:**	**……**

The persons present ask ..... to make the protocol of the Data access, who thankfully accepts the invitation. The protocol is authenticated with signature by the other members present.

Persons present coincidently fix that the Data subject in his/her letter/personal request/phone request/email dated to.....[3] has withdrawn his/her consent to management of personal data, and exercising his/her rights according to Decree 2016/679/EU of the European Parliament and the Council (hereinafter: "GDPR"), on the protection of management of personal data of natural persons, and on the flow of these data, as well as repealing 95/46/EC regulation (general data protection decree), and according to Act CXII of 2011 (hereinafter: "Infolaw") on the informational self-determination rights and the freedom of information *in particular, the Infolaw 17.§ par. (2)*, has requested the final deletion of the designated data.

Data affected with withdraw, deletion:

[2] In case of online data management e.g. e-mail address, username. In other cases, additional personal data managed by the Data Manager, required for identification, e.g. address, date of birth, etc.
[3] Please underline the appropriate section.

	Nature, scope, type of data	Data management purposes	Nature, method of data management	Data Manager and/or organizational unit of Data Manager with affected data management	Data transmission's circumstances (if appropriate)	Physical location of storage(1), designation of medium(s)	Type and nature of concerned archive - if archiving has taken place
1.							
2.							
3.							

Persons present coincidently ascertain that the deletion of the data above has not any hindrances – *based on neither legal nor authority inquiry, or in any other way besides the legitimate interest of the Data subject* – therefore, the necessary procedure(s) for the deletion, not affecting or if possible, not learning any other personal data - *unless this is impossible due to the nature of the deletion process* –, shall be carried out:

Operational process of data deletion:

Serial number of affected personal data	Description of deletion process, indicating the actual person performing the deletion
1.	
2.	
3.	

Any further relevant information during the data deletion, in regards with its circumstances: ..... ……

Description of additional circumstance(s) revealed during the data deletion: .....

The person present ...., as the legal representative of the Data Manager, undertakes to inform all recipients about the data deletion, with whom Data Manager has communicated personal data, unless this proves impossible or requires disproportionate effort. At the request of the Data subject, the Data Manager shall inform him/her about these recipients in writing.

The persons present do not wish to discuss anything else, therefore the Data Insight and certification protocol, after the signature of the persons present – *each page shall be signed* –, shall be adjourned at ..... hours and ..... minutes.

Date: ..... ., 2018. .....

Dated as above

_____ …… protocol-verifier

_____ …… protocol-verifier

_____ …… protocol maker

Annex No. 2:

D a t a p r o t e c t i o n i n c i d e n t s r e g i s t e r
– administered from 25 May 2018. –

APP Ltd.

Company Registration Number:	08-09-007336
Seat:	9028 Győr, Fehérvári Street 75.
Tax Number:	11611989-2-08
Electronic contact:	*info@diadem.com*
Phone:	96 / 512 910
Legal representatives:	Péter Csizmadia, Szilárd Csizmadia, Renáta Berkes, Alexandra Sinkó

as Data Manager (hereinafter "Data Manager").

The purpose of data protection incidents register:
The Data Manager, complying with the Act CXII of 2011 (hereinafter: "Infolaw") on the freedom of information and the Decree 2016/679/EU of the European Parliament and the Council (hereinafter: "GDPR"), on the protection of management of personal data of natural persons, and on the flow of these data, as well as repealing 95/46/EC regulation (general data protection decree), regarding data management covered by the Data Manager, fulfilling its obligations as per GDPR preamble par. (82), the Data Manager keeps a register of the data protection incidents, indicating facts related to the data management incident, its effects and remedies. This register allows the supervisory authority to verify the compliance of the Data Manager with the relevant legal requirements

On the basis of an inquiry, the Data Manager shall make this register available to the supervisory authority.

In annual breakdown, on the pages following this cover, the following data protection incidents have happened - up to the undersigned date - about which the Data Manager has learnt about:

Date: .....; 201.. .....

.....

.....
.....
Data Manager

List of data protection incidents
– Year 2018 –

	Date, duration of incident:	Circumstances by which the Data Manager has become aware of this:	Date of notification towards the NAIH:	Date of notification of Data subjects, in the absence of this, justification of ignorance:	Organizational unit concerned with the incident:	Scope of affected personal data	Scope and number of Data subjects affected with the data protection incident	Circumstances, effects of the data protection incident:	Measures taken to repel the data protection incident:	Other data defined in applicable law:	Other notes:
1.											
2.											
3.											
4.											
5.											
6.											
7.											
8.											
9.											
10.											
11.											
12.											
13.											
14.											
15.											
16.											
17.											
18.											
19.											
20											
21.											
22.											
23.											

Annex No. 3:

National Authority of Data Protection and Freedom Of Information
1125 Budapest,
Szilágyi Erzsébet alle 22/c.

or **Data subject**
Address

Subject: notification about data protection incident[4]

Dear ……..!

The undersigned, ..., as the contact representative (verified with authorization attached as Annex no. 1) of **APP Ltd.** (CRN.: 08-09-007336; 9028 Győr, Fehérvári Street 75.; tax number: 11611989-2-08) as Data Manager (hereinafter referred to as **Data Manager**), given that you and your personal data are affected with data management related to ..... by the Data Manager, fulfilling our obligations according to Act CXII of 2011 (hereinafter: "Infolaw") on the freedom of information and the Decree 2016/679/EU of the European Parliament and the Council (hereinafter: "GDPR"), on the protection of management of personal data of natural persons, and on the flow of these data, as well as repealing 95/46/EC regulation (general data protection decree) - in particular, but not exclusively that of GDPR section 2 article 34. –, without gratuitous delay, hereby

I inform you

about the following data protection incident that occurred at the Data Manager:

Description of data protection incident:

Nature, date of the data protection incident:	……..
Categories and approximate number of Data subjects:	*.....if possible.....*
Contact details:	*Address:* ..... *E-mail:* ..... *Phone:* ..... *Fax:* .....
Description of the likely consequences of the data protection incident:	……..
Measures planned or taken by the Data Manager to remedy a data protection incident, including, where appropriate, measures to mitigate any adverse consequences resulting from a data protection incident:	……..

I also inform you that the Data Manager has started the necessary security measures, whereby the rights to personal data of the Data subjects, including your personal data, are considered as a priority and are protected by all available means, and in case of unexpected failures we mitigate the extent of any possible harms.

I inform the respected Authority that we are not aware of any further information regarding the data protection incident; at the same time, we undertake to inform the respected Authority without delay, of any further knowledge or circumstance we learn about regarding the incident.[5]

The reason for this notification is the fact that, on the undersigned date, it cannot yet be certainly ruled out if the incident is likely to pose a high risk to the rights and freedoms of natural persons; regarding which we would like to ask you to wait for our next notification to inform you about the real extent of the risk of the incident and about the further necessary measures. If the risks presented by

[4] need to be adapted according to the notification of the Data subject and the supervisory authority
[5] relevant if related to the notification of the authority

the incident are considered insignificant and/or not affecting you, then we will notify you in in a short message with no comprehensive information.

Győr, _____

Annexes:

Annex no. 1: Authority of the contact

Hoping your understanding, I thank you in advance;

With all respect:

……
Data Manager

Annex No. 4:

C o n s e n t s t a t e m e n t
– for management of personal data –

I, the undersigned, ...

Birth name:	.....
Place and date of birth:	.....
Mother's maiden name:	.....
Address:	.....
Nationality:	.....

as adult person with legal capacity (hereinafter referred to as "Data subject"), by signing the present document

I d e c l a r e ,

that I have come to known the Data Management and Data Protection Regulations (hereinafter: Regulations) of **APP Ltd**., as Data Manager (hereinafter "Data Manager")

Company Registration Number:	08-09-007336
Seat:	9028 Győr, Fehérvári Street 75.
Tax Number:	11611989-2-08
Electronic contact:	info@diadem.com
Phone:	96 / 512 910
Legal representatives:	Péter Csizmadia, Szilárd Csizmadia, Renáta Berkes, Alexandra Sinkó

and I completely accept the Regulations - effective from the undersigned date -; also

I s p e c i f i c a l l y c o n s e n t

to the use, management, announcement to the authorities as per legal obligation, and transmission of the personal data provided by me to the Data Manager, until the fulfilment of the purposes declared in the Regulations.

In regards of the above, my consent is related to the Data Manager's following

.....	purpose
.....	title
.....	scope of relevant data *type, nature* –

data management, and in this context, it is to be considered related to the information and data generated by the Data Manager, as well.
By signing this document

I a c k n o w l e d g e t h a t

- in accordance with Act CXII of 2011 §21-22 on information self-determination right and the freedom of information, as well as according to the current data protection legislation in force, I may exercise my rights, I may request the rectification of the managed data, I can object against and request information about the data management, and I may request the deletion or locking of the data by post, or personally at the data center of the Data Manager, via phone or by e-mail.
- the data is stored and processed on paper and electronically.

Győr,

_____
Data subject

Before them, as witnesses:

Name: _____ **Name:** _____
Address: _____ **Address:** _____
Signature: _____ **Signature:** _____

Annex No. 5:

To APP. Ltd. data manager (hereinafter "Data Manager") Locally!
9028 Győr, Fehérvári Street 75.

Subject: Withdrawal of data management consent

Dear Data Manager!

I, the undersigned, **.....** (additional data required to identify[6]: .....), exercising my rights according to the Decree 2016/679/EU of the European Parliament and the Council (hereinafter: "GDPR"), on the protection of management of personal data of natural persons, and on the flow of these data, as well as repealing 95/46/EC regulation (general data protection decree) and according to provisions of Act CXII of 2011 (hereinafter: "Infolaw") on the right of self-determination and freedom of information - specifically as per Infolaw 17. § par. (2) - , hereby

I withdraw my consent regarding the management of my personal data and I request the deletion of my personal data

Data affected with withdraw, deletion:

- .....
- .....
- .....
- .....

I call the attention of the respected Data Manager to the fact that according to Infolaw 18. § (1), Data Manager has a further obligation to notify me and all those to whom previously the Data Manager forwarded my personal data for data management purposes.

According to Infolaw 18. § (2), if the Data Manager fails to comply with my request of deletion, it shall submit written or electronic notice of the factual and legal grounds for refusal of deletion, within twenty-five (25) days of the receipt of the request.

Please send the answer to the following address / e-mail address:

- .....

In the event of non-fulfilment of the statutory deletion obligation, as per Infolaw 52. § par. (1), any person may initiate an investigation at the National Data Protection and Information Freedom Authority, with reference to the fact that there has been a violation regarding personal data management, or its direct threat exists.

Győr, _____

Thank you in advance for your cooperation,

With all respect:

.....
Data subject

[6] In case of online data management e.g. e-mail address, username. In other cases, additional personal data managed by the Data Manager, required for identification, e.g. address, date of birth, etc.

Annex No. 6:

Confidentiality statement

In this statement our agreement is confirmed that the **APP Ltd.** On behalf of the Employer ..... *(employee's name, mother's maiden name, place and date of birth*) certain information disclosed and to be disclosed before me, as Employee (hereinafter Declarant), specifically business plans, trade secrets, customer information and other owner information, according to Act CXII of 2011 (hereinafter: "Infolaw") on the right of self-determination and freedom of information, these personal data (hereinafter referred to as "information") are confidential.

1. .....(employee's name) by signing the declaration, I agree that I will not disclose any part or all of the information, I will not provide it to any third party without the prior written consent of the authorized representative of APP Ltd., unless such information are disclosable as probative documents.
2. Such information shall not be considered to be disclosed merely because it may be used to obtain further general information, or they might be collected from one or more sources, or if the reason of their disclosure was because of the breach of this Declaration or similar statements were made with a third party or a legal person.
3. I hereby declare that I, as Declarant, will take all reasonable precautionary measures in order to adequately protect any such information disclosed orally, in writing, in an electronic storage medium or in any other way, against any unauthorized disclosure before any third party, in particular with respect to the provisions of the Employer's Data Protection and Data Security Regulations.
4. I undertake to make no copies of any material and return any copies of such materials immediately upon request.
5. As Declarant I also accept that all such information are owned by the Employer and that for the Company's ongoing business management, to ensure all this information is confidential, valuable and essential.
6. As Declarant, I declare that I will not use, exploit and/or commercialize such information for my own benefit or for any other third party.
7. The Parties hereby declare that signing the present Declaration by the Declarant does not entitle him/her to any other rights.
8. The Employer declares that the personal data in this confidentiality statement is managed in accordance with the Data Protection and Data Security Regulations.

Present confidentiality declaration comes into force as of ..... (date or specifically definable event, such as: "signing of employment contract").

Győr, _____

_____	_____
Employee Declarant	Employer Data Manager