Privacy Policy

updated January 17, 2018

1 Introduction

Cellum Global Zrt. (Address: 6725 Szeged, Pálfy utca 46., Hungary; Registry no.: Cg.: 14-10-300278, Tax no.: 23471625-2-06), hereinafter referred to as "Cellum", "supplier", or "data handler"), in its capacity as a data manager and/or data processor

1. agrees to be bound by the stipulations of this privacy policy;
2. warrants that its data management and/or processing operations, rendered in connection with its services, shall comply with the requirements set forth in this privacy policy and in other relevant legislation;
3. reserves the right to amend this privacy policy at its own discretion at any time, in which case it will publish an appropriate announcement relating to the concerned amendments on the **www.cellum.com** website;
4. is committed to the protection of the personal data of its partners and users, and holds in high regard its clients' right to informational self-determination;
5. manages and/or processes the submitted personal data confidentially and takes all security, technological and organizational measures in order to guarantee the security of such data ("**data security**");
6. publishes its data management and/or processing principles in this document and presents the requirements that it has set forth for itself as a data manager and/or (as the case may be) data processor, and which it abides by;
7. declares, that its privacy policy is in compliance with the applicable data protection legislation at all times;
8. by reading this Privacy Policy and/or using Cellum's services, you agree to be bound by it.

2 Principles

2.1. During Cellum's data management and/or processing procedures, personal information can only be managed and/or processed if

i. the concerned party has given its consent to it, or

ii. for the sake of public interest, it is made compulsory by (a) an act of law or, based on the act of law and within the scope that such law defines, (b) a municipal regulation ("**complusory data handling**").

2.2. Personal information can only be managed and/or processed for a definite purpose, for the sake of exercising rights and completing obligations. Data management and/or processing shall comply with the purpose of the data handling at all instances.

2.3. Only personal information that is indispensable and suitable for attaining the goal of the data management and/or processing can be managed and/or processed, and only to the extent and up to the period of time that is necessary for achieving such purpose.

2.4. Personal information can only be managed and/or processed with the client's consent granted based on an adequate notice. The concerned party shall be informed in a clear, articulate and detailed manner on every aspects concerning the management and/or processing of his/her data, in particular the purpose and legal basis of the data management and/or processing, the entities allowed to manage and process the data, the duration of the data management and/or processing, and the entities to whom the data can become known. The notice must also cover the rights of the concerned party relating to the management and/or processing of his/her data, and his/her possibilities for legal remedy. Personal data must meet the following criteria in order to properly qualify for data management and/or processing:

i. they have been recorded, and are managed and/or processed in a fair and lawful manner;

ii. they are accurate, complete and, provided it is necessary for the purpose of the data management and/or processing, up to date;

iii. the concerned party can only be identified for the time period that is necessary for the purpose of the data management and/or processing.

2.5. It is forbidden to use any personal identifier that is common, uniform and can be used without limitation.

2.6. Personal data can be forwarded to any third parties, and different data management and/or processing can be linked together only if the concerned party has given its consent thereto, or it is permitted by the rules of law, and if the requirements and conditions for the data management and/or processing are met for each piece of personal data.

2.7. Personal data (including out-of-the-common personal data) – regardless to the type of data storage or transferring method – can only be transferred to a third-country data manager or data processor if the concerned party has given its express consent thereto, or if it is permitted by the rules of law, and further, if an adequate level of protection is ensured for the personal data during the management and processing of the transferred data in that third country.

2.8. Data transfer to member states of the European Economic Area shall be considered as if it was data transfer within the territory of Hungary.

3 Scope of personal data, objective, ground and duration of data management and/or processing

3.1. All data management and/or processing relating to the concerned party, taking place as part of Cellum's various services shall be based on the voluntary consent of the concerned party.

3.2. Data management and/or processing in relation to mobile payment (technical) services

3.2.1. Cellum shall, during the course of providing its various mobile payment (technical) services to a corresponding white label wallet of a wallet-provider, (A) process (in its capacity as data processor), and within this scope, (B) transmit to (a) the merchants and (c) acquirer banks/financial institutions, participating in the clearance and completion of the given mobile payment transaction, the following personal data only, provided by the end-user through the corresponding client side mobile application platform. Such data shall be processed merely for the purpose of (i) using the corresponding mobile transaction/payment service by the end-user of the service, (ii) completing and (iii) tracking down the transactions by the entities/service providers, participating in the relevant solution's architecture:

i. the mobile phone number of the service user;

ii. the card number, security code (CVV2/CVC2/CSC = the 3-digit number next to the signature field on the back of the bank card, or the PCSC, which is a 4-digit number on the front) and the maturity (i.e.: "Good Thru") date of the bank card of the service user;

iii. the name of the service user (as it appears on the bank card);

iv. e-mail address, delivery address and billing address.

3.2.2. These data are stored by Cellum until the service user deletes them from the mobile phone, or until the bank card expires. In these events, the data listed in section 3.2.1 are deleted from the system.

3.2.3. In accordance with the above, Cellum sends to the service user's mobile phone the notifications as well as the information about the transactions, as specified in the General Terms and Conditions.

3.3. Personal data of visitors to Cellum's website

3.3.1. Cellum's website, **cellum.com** can be visited – subject to the provisions set out in Sections 3.4 and 3.5 – without giving away any kind of personal data. The visitor can learn about Cellum's services through the website.

3.3.2. In order for Cellum to be able to provide personalized services to the visitor, Cellum may place a data package called cookie on the visitor's computer, in order to be able to remember the settings saved by the visitor. The visitor can delete the cookie anytime or set his/her browser to block cookies.

3.3.3. Cellum uses Universal Analytics by Google to analyze traffic to and on its website. Universal Analytics uses "cookies" to collect statistics on how visitors use the website, which helps Cellum to improve its website's user experience. Such statistics are anonymized and do not concern any personal data of users of mobile payment applications developed by Cellum. Detailed information on Universal Analytics is available from Google. URL: **https://support.google.com/analytics/answer/2838718**.

3.4. Email marketing service

3.4.1. Visitors can subscribe to Cellum's email marketing service on Cellum's website. Cellum sends emails about its latest news and offers to users who have opted in or consented to receiving these emails.

3.4.2. In order to provide the email marketing service, Cellum requires subscribers to provide certain personal data using a dedicated form, including but not limited to: name, e-mail address, country, and business segment. The provision of these data by the subscriber is voluntary and based on the subscriber's explicit consent. Cellum does not collect any other information about subscribers than those, set out above.

3.4.3. Cellum may use third-party service providers to provide the email marketing service. This includes the storage of subscriber data, analytics and content personalization, using parties located in third countries. These third parties are listed in Section 6.1.

3.4.4. Visitors who wish to subscribe to Cellum's email marketing service are duly notified on the dedicated subscription form before submitting their personal data that their personal data shall become transferable to the third parties described in Section 3.4.3, for the sole purpose of sending the marketing emails, pursuant to the conditions set out in Section 2.7 above. A visitor may only subscribe to the email marketing service if he/she explicitly approves such transfer of his/her personal data, set out in Section 3.4.2 above. Cellum undertakes to ensure that the name, country and email address of the subscriber is transferred only to a third-country data manager and/or data processor whose country of location guarantees due level of protection of the transferred personal data during the management and processing.

3.4.5. The personal data submitted by subscribers pursuant to Section 3.4.2 will only be used by Cellum for the intended purpose, namely for providing the email marketing service. Cellum will not forward or sell these data, with the exception stated in Section 3.4.3, to any third parties, not including the members of the company group, without the knowledge and consent of the subscriber. The content of individual emails may vary depending on the data provided by the subscribers.

3.4.6. Cellum may include in its marketing emails offers from other Cellum group companies as well as that of Cellum's clients.

3.4.7. Cellum provides the possibility to unsubscribe from the email marketing service at any time. After unsubscribing, no personal data of the subscriber shall be managed anymore by Cellum, and those data will be destroyed within a reasonable time.

3.5. Data handling concerning Cellum's restricted access PR, demo and other marketing purpose materials

3.5.1. Cellum publishes certain exclusive content, such as PR, demo and marketing purpose materials, that is available only to subscribers of the email marketing service detailed in Section 3.4. These restricted resources may only be copied and redistributed with the written express consent of Cellum.

3.5.2. In order to access these restricted resources, visitors must first subscribe to Cellum's email marketing service by providing certain personal data, as described in Section 3.4.2. Furthermore, Cellum also records the title of the downloaded resource.

3.6. Data management and/or processing for the purpose of keeping contact

3.6.1. Visitors can contact Cellum via e-mail using the contact form on its website.

3.6.2. In order to contact Cellum using the contact form, the visitor must fill out the contact form with his/her personal data, including but not limited to: name, country and e-mail address.

3.6.3. Personal data submitted in the above way shall be used by Cellum only for the specific goal requested by the visitor, and will not be used to provide the email marketing service detailed in Section 3.4. Cellum will not transfer or sell such personal data to third parties – not including members of the company group – without the consent of the concerned party.

3.6.4. Cellum will archive the above personal data following the final resolution of the matter and will store them for a period of no more than one (1) year from the date of submission.

3.7. Data management and/or processing related to Cellum's clients

3.7.1. Personal data submitted by clients shall be used by Cellum only for the intended business purpose. Cellum will not transfer or sell such personal data, with the exceptions stated in Section 6.1, to third parties – not including members of the company group – without the knowledge and consent of the concerned party.

3.7.2. The data in question shall be destroyed by Cellum once the client relationship is terminated.

3.8. Miscellaneous data management and/or processing

3.8.1. In the case of any other type of data management and/or processing activities not listed in this document, Cellum will provide complete information when recording the data from the user/client.

3.8.2. Cellum hereby informs all concerned parties that pursuant to Article 71.§ of the Act no.: XIX. of 1998 on Criminal Procedure, courts, public prosecutor's offices and investigation authorities may contact Cellum requiring the handover of information, the dissemination/transmission of data, and the provision of documents, by setting a minimum eight (8), maximum thirty (30) days compliance deadline. Cellum is obligated to restore all encrypted or other data made unreadable for human eyes in any other manner into its original form before the handover, and make the content of the data accessible to the inquiring party. Cellum is required, unless otherwise provided by law, to comply with the inquiry within the set deadline or state the reason of its hindrance.

3.8.3. Cellum will hand over personal data – provided that the authority has indicated specifically in its inquiry the exact objective and the scope of data – exclusively to the authorized authorities, and only to the extent that is essential for the purpose of achieving the objective of the given inquiry.

4 Data storage, data security

4.1. The user's personal data are stored in an environment supervised by Cellum. Cellum's information technology systems are supported by Cellum Zrt. (address: Puskás Tivadar út 14. C/B, 2040 Budaörs, Hungary) and MPP Zrt. (address: Puskás Tivadar út 14. C/B, 2040 Budaörs, Hungary). These organizations can only access data managed by Cellum in their quality as data processors and/or subordinated data processors.

4.2. For data management and/or processing, Cellum chooses and operates the equipment used while providing its service in a way that ensures that the managed and/or processed data:

i. can be accessed only by the authorized parties (availability);

ii. is authentic and authenticated (authenticity of data management and/or processing);

iii. its uniformity can be verified (data integrity);

iv. is protected against unauthorized access (data confidentiality, see section 4.4 below).

4.3. During its data management and/or processing procedures, Cellum ensures that data shall always be kept

i. secret: as per the above, it protects the information so that only authorized parties can access them;

ii. uncompromised: it protects the accuracy and completeness of the information and the method of processing;

iii. available: it ensures that the authorized user can access the required information within reasonable time, whenever he/she needs to, by using the equipment available for this purpose.

4.4. Cellum's information technology system and network are protected against computer fraud, espionage, sabotage, vandalism, fire and flood, as well as computer viruses, hacker attacks and denial-of-service attacks. The system operator ensures security with server-side and application-side protection methods.

4.5. Cellum hereby advises users that messages sent over the internet and/or mobile networks, regardless to the applied protocol (e.g.: e-mail, web, ftp, SMS, MMS, push, etc.) are vulnerable to threats that strive for or lead to fraudulent activity, the questioning of the validity/effectiveness of a contract, or aim to solicit or modify information. Cellum will take every precaution it can in order to prevent such threats, including the continuous upgrading of its systems, as well as maintaining its PCI DSS compliance and certificate.

5 Details and contact information of the data manager

5.1. Name: **Cellum Global Zrt.**
5.2. Address: Pálfy utca 46., 6725 Szeged, Hungary
5.3. Company registry number: Cg.: 14-10-300278
5.4. Tax number: 23471625-2-06
5.5. Email: contact@cellum.com

6 Data forwarding

6.1. Cellum, pursuant to Sections 3.4, 3.5, 3.6 and 3.7 above, will forward the personal data of concerned parties to the following enterprises/subcontractors, and only for the purpose of (i) providing the email marketing service:

i. name of the data processor: **Cellum Zrt.**
address: *Puskás Tivadar út 14. C/B, 2040 Budaörs, Hungary*

ii. name of the data processor: **The Rocket Science Group, LLC**
address: *675 Ponce de Leon Ave NE, Suite 5000, Atlanta, GA 30308 USA*
contact form: https://mailchimp.com/contact/

iii. scope of the personal data transfer: the user's (i) name, (ii) e-mail address, (iii) company name, (iv) business segment, (v) position held and (vi) country.

iv. purpose of the personal data transfer: providing the email marketing service. The user may unsubscribe and/or opt out via email or a dedicated online form, without further conditions, at any time.

6.2. Cellum, in relation to the mobile payment service outlined in Section 3.2 will forward the personal data of the concerned parties to the following enterprises/subcontractors, and only for the purpose of providing the newsletter services:

i. Name of data manager(s) (1): the acquirer bank(s) or financial institution(s), participating in the acceptance/clearing of the transactions;

ii. Address of the data manager(s) (1): as it/they is/are set forth in the webpage of, or the contractual documentation relating to the mobile payment service;

iii. Name of data processor(s) (2): the merchant(s), participating in the clearing of the transactions;

iv. Address of the data processor(s) (2): as it/they is/are set forth in the webpage of the integrated merchant, or the contractual documentation relating to such service;

v. Name of the subordinated data processor (3): **MPP Zrt.**;

vi. Address of the data processor (3): *Puskás Tivadar út 14. C/B, 2040 Budaörs, Hungary*;

vii. Scope of forwarded data:

a) the mobile phone number of the service user;

b) the card number, security code (CVV2/CVC2/CSC = the 3-digit number next to the signature field on the back of the bank card, or the PCSC, which is a 4-digit number on the front) and the maturity (i.e.: "Good Thru") date of the bank card of the service user;

c) the name of the service user (as it appears on the bank card);

d) e-mail address, delivery address and billing address.

viii. Purpose of forwarded data: to carry out mobile payment transactions, and to monitor user transactions with the intent of customer care, both by the actual wallet provider.

7 Legal remedy

7.1. The concerned party may ask to be informed about the management and/or processing of his/her personal data or – with the exception of the limitations set forth in the relevant legislation – may request that Customer Service delete such data, or can also personally do so by removing these data from his/her mobile phone. The concerned party understands that – given the absence of his/her personal data necessary for identifying the underlying bank cards behind the service – In the case of deleting or destroying his/her personal data in any of the above manner, he/she will not be able to use Cellum's mobile payment services following to successful deletion.

7.2. Upon request from the concerned party, Cellum, in its capacity as data manager, shall provide information on (i) the personal data managed by it or forwarded to a data processor for processing, as well as on the (ii) purpose, (iii) legal basis (iv) duration of the data management and/or processing, (v) on the name and (vi) address of the data processor, (vii) its activities related to the data management and/or processing, and on (viii) who and for what purpose has received or will receive the said data. The data manager shall provide a written and common sense language response to the request within the shortest possible deadline, but no later than within thirty (30) days following to the date of the request. In case the party concerned does not speak Hungarian, the information shall be provided in English. Provided that the requesting party has not submitted another request for the same scope of data to the data manager in the current year, the granting of the above information will be free. The requiring party agrees that the data manager shall be entitled to bill for its costs and expenses to the requiring party in any other cases.

7.3. Cellum shall delete personal data if the management and/or processing thereof is illegal, if it is requested by the concerned party, if the purpose of the data management and/or processing is terminated, if the deadline set by the law for the data management and/or processing expires, or if it is required by Court or the National Data Protection and Information Freedom Authority of Hungary.

7.4. Cellum informs the concerned party about the correction or deletion of these data, as well as all other parties whom the data were previously forwarded to for the purpose of data management and/or processing. Such notification may be omitted if, with regard to the purpose of the data management and/or processing, it does not infringe the rightful interest of the concerned party.

7.5. The party concerned may petition against the management and/or processing of his/her personal data if

i. the management or forwarding of personal data is necessary only for the fulfilment of the legal obligations or the pursuit of the rightful interests of the data manager or data recipient, unless the management and/or processing of data is required by law ("mandatory data management");

ii. the personal data is used or handled for the purpose of securing business, opinion polling or scientific research;

iii. the right to petition is otherwise provided by the law.

7.6. Cellum (i) will examine the petition within the shortest possible deadline, but no later than within fifteen (15) days from the date of receiving the petition, (ii) will inform the requesting party in writing whether or not the petition has been found to be substantiated, and simultaneously to all this (iii) will suspend the related data management and/or processing activities. In case the petition is found to be substantiated, the data manager – including any further data recording and -forwarding activities – will discontinue the management and/or processing of the data will block the data and will inform all parties about the petition and the subsequent actions, whom the personal data subject to the petition were previously sent to, and who are required to take action in order to enforce the said right to petition.

7.7. In case the requesting party disagrees with Cellum's decision, he/she can apply to the Courts within thirty (30) days from the date of reception of Cellum's notice.

7.8. Cellum may not delete the data of the concerned party if its management and/or processing was stipulated by law (mandatory data management and/or processing). Notwithstanding the above, those data cannot be forwarded to the recipient if the data manager agrees with the petition, or if the Court has ruled the petition to be justified.

7.9. In case the rights of the concerned party are infringed, he/she may apply to the Courts. The Court shall be acting out of turn. Cellum will, based on the Court's ruling, indemnify the party concerned for damages due to illegal management and/or processing of private data or failure to meet data security requirements.

7.10. The data manager shall be responsible for damages caused by the data processor towards the concerned party. The data manager shall be exempt from liability if the damage was caused by unforeseeable circumstances beyond the scope of the data management and/or processing (force majeure). Damages need not be indemnified for to the extent they have been caused by will or gross negligence of the injured party.

7.11. Complaints related to Cellum's management and/or processing of data can be submitted to the **National Data Protection and Information Freedom Authority** (NAIH), via one of the following:

- Address: *1125 Budapest, Szilágyi Erzsébet fasor 22/c.*
- P.O. box: 1530 Budapest, Pf.: 5.
- Phone no.: +36 1 391 1400
- Fax no.: +36 1 391 1410
- E-mail: ugyfelszolgalat@naih.hu

7.12. Cellum provides its data management (and/or corresponding -processing) activities under the following Licenses from the National Data Protection and Information Freedom Authority (NAIH):

(i) Description of the data management: "*Mobil fizetési szolgáltatás üzemeltetése. a mobiltelefonra telepített alkalmazás segítségével történő bankkártyás fizetés (mobil fizetési szolgáltatás) lebonyolítása*." Registration number: **NAIH-74782/2014.**

(ii) Description of the data management: "*Hírlevél küldési szolgáltatás, korlátozott elérésű PR, demó és egyéb anyagok letöltési lehetőségének, illetőleg ügyintézési célú, közvetlen kapcsolatfelvétel lehetőségének biztosítása. a Cellum Global Zrt. honlapjára látogató ügyfélnek lehetősége nyílik feliratkozni a Cellum Global Zrt, hírlevél-küldő szolgáltatására, a Cellum Global Zrt, honlapjáról illetőleg ezen célra meghatározott felületeiről korlátozott elérésű PR, demó és egyéb anyagok közvetlenül letölteni, valamint a Cellum Global Zrt-vel ügyintézési célzattal közvetlenül kapcsolatba lépni.*" Registration number: **NAIH-76853/2014.**

(iii) Description of the data management: "*Marketing célú, közvetlen kapcsolatfelvételt lehetőségének biztosítása. a (a) Cellum Global Zrt. honlapjára, lehetőleg (b) a Network Media Group (13100 Eastpoint Park Blvd., Louisville, KY 40223 USA) által működtetett 'Mobile Payment Today' honlapra látogató, és alábbi 6.1. illetőleg 7.1 pontban meghatározott adatait megadó ügyféladatok alapján a Cellumnak lehetősége nyílik az ügyfelet marketing, illetőleg értékesítés céljából közvetlenül megkeresni.*" Registration number: **NAIH-78509/2014.**

8 Definitions

Terms used in this Privacy Policy are defined as follows:

- "**personal data**": means any data that can be associated with any specific (identified or identifiable) natural person ("concerned party"), or implications that can be inferred from such data relating to the concerned party. Data shall maintain its personal quality throughout the data management and/or processing process so long as its connection with the concerned party can be restored. A person can be considered identifiable in particular if he/she can directly or indirectly be identified based on any traits relating to his/her (i) name, (ii) identification number, or one or more (iii) physical, (iv) physiological, (v) mental, (vi) economic, (vii) cultural or (viii) social identity.
- "**approval**": means the voluntary and explicit expression, based on adequate information, the concerned party's will, by which he/she gives unequivocal consent to the comprehensive or partial management and/or processing of his/her personal data.
- "**petition**": means a declaration from the concerned party expressing disapproval of the management and/or processing of his/her personal data and requesting the discontinuation of the data management and/or processing and/or the deletion of the managed and/or processed data.
- "**data manager**": means a natural or legal person, or an organization without legal personality, who/that determines the purpose of the data management, makes decisions (including the used equipment) regarding the data management and executes, or has the data processor to execute them.
- "**data management**": means, regardless to the procedure applied, any or all actions performed on/with the data, such as (i) collecting, (ii) recording, (iii) saving, (iv) sorting, (v) storing, (vi) modifying, (vii) using, (viii) forwarding, (ix) publishing, (x) according or joining, (xi) blocking, deleting and destroying said data, as well as (xii) the prevention of its further use. Photographing, sound or video recording, and sampling physical traits suitable for the identification of the person (e.g. finger- or palm prints, DNS sample, iris image) shall also qualify data management activity.
- "**data forwarding**": means when the data is made available to a specified third party.
- "**publishing**": means when the data is made available to anyone.
- "**data deletion**": means making the data unrecognizable in a way that it cannot be restored anymore.
- "**data blocking**": means the marking the data with an identifier in order to permanently or temporarily limit its further management.
- "**data destruction**": means the complete physical destruction of the storage device holding the data.
- "**data processing**": means the performing of technical tasks related to the data management processes, regardless to the methods and tools applied and/or the location where it takes place.
- "**data processor**": means a natural or legal person or an organization without legal personality that processes the data on behalf of the data manager.
- "**third party**": means a natural or legal person or an organization without legal personality that is not identical to the concerned party, the data handler, or the data processor.
- "**third country**": means a country that is not a member of the European Economic Area.
- "**EEA country**": means a member of the European Union or a party to the agreement on the European Economic Area, or a country whose citizens, based on an international treaty between the European Union and its member states on the one hand, and the country that is not party to the agreement on the European

Economic Area on the other hand, enjoy the same legal status as the citizens of a state that is party to the agreement on the European Economic Area.

- "**concerned party**": any specific natural person identified or – directly or indirectly – identifiable based on personal data.