

Data Processing Agreement • Adatfeldolgozási szerződés

Version 1.0 · Effective from 17 October 2026 · Downloadable: [PDF](#)

1. Parties and conclusion

This Data Processing Agreement (“DPA”) is concluded between the customer using the QR Lead Capture service (the “Customer”, controller) and **Fluid Digital Kft.** (4400 Nyíregyháza, Könyves utca 2/a, Hungary; company reg. no. 15-09-090475; tax no. 32079867-2-15; “Fluid Digital”, processor), pursuant to Article 28 of Regulation (EU) 2016/679 (GDPR).

The DPA forms an integral part of the [Terms of Service](#) (“TC”) and of any individual contract, and is accepted together with them. On request, Fluid Digital also signs it as a separate document. In data protection matters this DPA prevails over the TC and any other agreement between the parties.

2. Subject and duration

Fluid Digital processes personal data on behalf of the Customer solely to provide the QR Lead Capture service. The subject matter, nature, purpose, types of

personal data and categories of data subjects are set out in [Annex 1](#). The DPA applies for as long as Fluid Digital processes personal data on behalf of the Customer.

3. Instructions

Fluid Digital processes personal data only on documented instructions from the Customer, including with regard to transfers to third countries, unless EU or Hungarian law requires otherwise; in that case it informs the Customer before processing, unless the law prohibits it. The TC, this DPA, the Customer's settings and use of the service, and the Customer's written (including e-mail) requests constitute the Customer's instructions. Fluid Digital immediately informs the Customer if, in its opinion, an instruction infringes data protection law.

4. Confidentiality

Fluid Digital ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under a statutory obligation of confidentiality, and access the data only as needed for the service, support or maintenance.

5. Security

Fluid Digital implements the technical and organisational measures in [Annex 2](#) in accordance with Article 32 GDPR. It may update them as long as the level of protection is not reduced.

6. Sub-processors

The Customer gives general authorisation to engage the sub-processors listed in [Annex 3](#). Fluid Digital informs the Customer of any intended addition or replacement at least 30 days in advance, by e-mail or by updating Annex 3 on this page. The Customer may object on reasonable data protection grounds within that period; if the parties cannot agree, the Customer may terminate the affected service with immediate effect and receive a pro-rata refund of prepaid fees. Fluid Digital imposes on each sub-processor data protection obligations equivalent to this DPA, and remains fully liable to the Customer for the sub-processor's performance.

7. Transfers outside the EU

Personal data is stored in the EU. As listed in Annex 3, some processing takes place in the USA: the app's login function and crash reporting (Google LLC). These transfers are based on the EU–US Data Privacy Framework adequacy decision (Google LLC is certified) and the Standard Contractual Clauses included in Google's data processing terms. The Customer authorises these transfers. Fluid Digital does not make any other transfer to a third country without the Customer's instruction.

8. Assistance

Taking into account the nature of the processing, Fluid Digital assists the Customer (a) by appropriate technical and organisational measures in responding to data subjects' requests (Articles 12–23 GDPR) – requests received directly are forwarded to the Customer without undue delay and are not answered by Fluid Digital on its own; and (b) in ensuring compliance with Articles 32–36 GDPR (security, breach notification, data protection impact assessment, prior consultation), using the information available to it.

9. Personal data breaches

Fluid Digital notifies the Customer without undue delay, and in any case within 48 hours after becoming aware of a personal data breach affecting the Customer's data, providing the information required by Article 33(3) GDPR as far as available, and supplements it as it becomes available. Fluid Digital takes the necessary measures to contain the breach and mitigate its effects.

10. Deletion and return

Event data (install codes, leads, logo, badge files) is deleted automatically 90 days after the end date of the event. Until then the Customer can export its data from the application (CSV/XLSX). At the end of the service, Fluid Digital, at the Customer's choice, returns the personal data or deletes it, at the latest within 90 days, unless EU or Hungarian law requires its storage. Earlier deletion can be requested at info@qrleadcapture.com.

11. Information and audits

Fluid Digital makes available to the Customer all information necessary to demonstrate compliance with Article 28 GDPR, primarily through this DPA, its annexes, and written answers to the Customer's questions. It allows for and contributes to audits, including inspections, by the Customer or an auditor mandated by it and bound by confidentiality, with at least 30 days' written notice, during business hours, without disrupting operations, normally no more than once a year (unless required by a supervisory authority or following a breach), at the Customer's cost. Audits of Google's infrastructure are satisfied by Google's independent certifications and reports (e.g. ISO/IEC 27001, 27017, 27018, SOC 2).

12. Liability and final provisions

Each party's liability towards data subjects is governed by Article 82 GDPR. Between the parties, the liability rules of the TC apply to the extent permitted by law. This DPA is governed by Hungarian law; the court designated in the TC has jurisdiction. If any provision is invalid, the remaining provisions remain in force. The Hungarian version is a translation; in case of discrepancy the English version prevails.

Annex 1 – Details of processing

Subject matter and nature	Hosting and operation of the QR Lead Capture mobile app and admin portals: collection (scanning, manual entry), storage, display, export and deletion of data.
Purpose	Enabling exhibitors to capture and manage leads at events, and organizers to manage exhibitors and install codes.
Categories of data subjects	Event visitors and other contacts whose data is captured (leads); exhibitor staff using the app; contact persons of exhibitors uploaded by organizers.
Types of personal data	Leads: name, e-mail, phone number, company, job title, address, website, social profiles, notes, category, custom fields, time of capture. Exhibitors: name, e-mail, company, install code, device names, number of devices.
Special categories	None intended. The Customer must not record special categories of data (Article 9 GDPR) in free-text fields.
Frequency	Continuous, for the duration of the service.

Retention	Until 90 days after the end date of the event, or earlier deletion on the Customer's instruction.
Location	Storage: Google Cloud EU (Belgium, the Netherlands). Processing: EU; and the USA as listed in Annex 3.

Annex 2 – Technical and organisational measures (TOMs)

- **Encryption:** all connections use TLS (HTTPS); data at rest is encrypted by Google Cloud (AES-256).
- **Access control – app:** users authenticate with an install code; database security rules ensure each exhibitor can only read and write its own leads.
- **Access control – portals:** organizer portal access only for the e-mail address assigned to the event; system administration limited to a named allowlist of administrators, protected by password and two-factor authentication (TOTP).
- **Least privilege:** service accounts have only the roles they need; credentials and keys are not stored in source code.
- **Segregation:** data is logically separated per event and per exhibitor.
- **Data minimisation and deletion:** automatic deletion 90 days after the end date of the event; only the data needed for the service is collected.
- **Logging and monitoring:** technical logs in Google Cloud Logging (30 days); crash monitoring via Firebase Crashlytics.
- **Infrastructure:** Google Cloud data centres with physical security, redundancy and independent certifications (ISO/IEC 27001, 27017, 27018, SOC 2).
- **Change management:** code changes via version control and reviewed pull requests; automated deployments.
- **Personnel:** confidentiality obligations; access only for staff who need it.
- **Incident handling:** documented breach procedure; Customer notification within 48 hours (section 9).

Annex 3 – Sub-processors

Sub-processor	Service	Location	Transfer safeguard
Csomós Róbert e.v. (Hungary, 4183 Kaba, Liget utca 8.)	Development and operation of the service; contracts the Google Cloud services listed below	EU – Hungary	–
Google Cloud EMEA Ltd. (Ireland)	Hosting, database (Cloud Firestore), file storage, backend services, admin portals (Google Cloud / Firebase)	EU – Belgium, the Netherlands, Poland	–
Google LLC (USA)	App login function (reads exhibitor name and e-mail, stores nothing); Firebase Authentication (global service); Firebase Crashlytics crash reports (no lead data)	USA / global	EU-US Data Privacy Framework; Standard Contractual Clauses
Google Ireland Ltd. (Ireland)	Company e-mail (Google Workspace), used for support communication	EU / global	Standard Contractual Clauses

Last updated: 17 October 2026.

Adatfeldolgozási szerződés

1.0 verzió · Hatályos 2026. október 17-től · Letölthető: [PDF](#)

1. Felek és a szerződés létrejötte

Jelen adatfeldolgozási szerződés („Szerződés”) a QR Lead Capture szolgáltatást igénybe vevő ügyfél („Ügyfél”, adatkezelő) és a **Fluid Digital Kft.** (4400 Nyíregyháza, Könyves utca 2/a; cégjegyzékszám: 15-09-090475; adószám: 32079867-2-15; „Fluid Digital”, adatfeldolgozó) között jön létre az (EU) 2016/679 rendelet (GDPR) 28. cikke alapján.

A Szerződés az Általános Szerződési Feltételek („ÁSZF”) és az egyedi szerződések elválaszthatatlan része, azokkal együtt kerül elfogadásra. Kérésre a Fluid Digital külön dokumentumként is aláírja. Adatvédelmi kérdésekben jelen Szerződés elsőbbséget élvez az ÁSZF-fel és a felek közötti más megállapodással szemben.

2. Tárgy és időtartam

A Fluid Digital a személyes adatokat az Ügyfél megbízásából, kizárólag a QR Lead Capture szolgáltatás nyújtása céljából kezeli. Az adatkezelés tárgyát, jellegét, célját, a személyes adatok típusait és az érintettek kategóriáit az 1. melléklet tartalmazza. A Szerződés addig hatályos, ameddig a Fluid Digital az Ügyfél megbízásából személyes adatot kezel.

3. Utasítások

A Fluid Digital a személyes adatokat kizárólag az Ügyfél dokumentált utasításai alapján kezeli, ideértve a harmadik országba történő továbbítást is, kivéve, ha uniós vagy magyar jog ettől eltérő kezelést ír elő; ilyenkor erről az adatkezelés előtt tájékoztatja az Ügyfelet, hacsak jogszabály ezt nem tiltja. Az Ügyfél utasításának minősül az ÁSZF, jelen Szerződés, az Ügyfél beállításai és szolgáltatáshasználata, valamint írásbeli (e-mailes) kérése. A Fluid Digital haladéktalanul jelzi, ha megítélése szerint egy utasítás sérti az adatvédelmi jogszabályokat.

4. Titoktartás

A Fluid Digital biztosítja, hogy a személyes adatok kezelésére feljogosított személyek titoktartást vállaltak vagy jogszabályi titoktartási kötelezettség alatt állnak, és az adatokhoz csak a szolgáltatáshoz, ügyfélszolgálathoz vagy karbantartáshoz szükséges mértékben férnek hozzá.

5. Adatbiztonság

A Fluid Digital a GDPR 32. cikkének megfelelően a 2. mellékletben felsorolt technikai és szervezési intézkedéseket alkalmazza. Ezeket frissítheti, ha a védelem szintje nem csökken.

6. További adatfeldolgozók

Az Ügyfél általános felhatalmazást ad a 3. mellékletben felsorolt további adatfeldolgozók igénybevételére. A Fluid Digital a tervezett bővítésről vagy cseréről legalább 30 nappal előre tájékoztatja az Ügyfelet e-mailben vagy a 3. melléklet ezen az oldalon történő frissítésével. Az Ügyfél ezen határidőn belül észszerű adatvédelmi okból tiltakozhat; ha a felek nem tudnak megállapodni, az Ügyfél az érintett szolgáltatást azonnali hatállyal felmondhatja, és az előre kifizetett díj időarányos részét visszakapja. A Fluid Digital minden további adatfeldolgozóra jelen Szerződéssel egyenértékű adatvédelmi kötelezettségeket ró, és a további adatfeldolgozó teljesítéséért teljes felelősséggel tartozik az Ügyfél felé.

7. Adattovábbítás az EU-n kívülre

A személyes adatokat az EU-ban tároljuk. A 3. mellékletben felsoroltak szerint egyes adatkezelések az USA-ban történnek: az alkalmazás bejelentkezési funkciója és a hibajelentés (Google LLC). Ezek alapja az EU–USA adatvédelmi keretrendszerrel szóló megfelelőségi határozat (a Google LLC tanúsított) és a Google adatfeldolgozási feltételeiben foglalt általános adatvédelmi kikötések (SCC). Az Ügyfél ezeket a továbbításokat engedélyezi. Más harmadik országba történő továbbítást a Fluid Digital az Ügyfél utasítása nélkül nem végez.

8. Közreműködés

Az adatkezelés jellegét figyelembe véve a Fluid Digital segíti az Ügyfelet a) megfelelő technikai és szervezési intézkedésekkel az érintetti kérelmek megválaszolásában (GDPR 12–23. cikk) – a közvetlenül hozzá érkező kérelmeket indokolatlan késedelem nélkül továbbítja az Ügyfélnek, és azokra önállóan nem válaszol; valamint b) a GDPR 32–36. cikkében foglalt kötelezettségek (adatbiztonság, incidensbejelentés, adatvédelmi hatásvizsgálat, előzetes konzultáció) teljesítésében, a rendelkezésére álló információk alapján.

9. Adatvédelmi incidensek

A Fluid Digital az Ügyfél adatait érintő adatvédelmi incidensről indokolatlan késedelem nélkül, de legkésőbb a tudomásszerzéstől számított 48 órán belül értesíti az Ügyfelet, megadva a GDPR 33. cikk (3) bekezdése szerinti, rendelkezésre álló információkat, és azokat folyamatosan kiegészíti. Megteszi a szükséges intézkedéseket az incidens elhárítására és következményeinek enyhítésére.

10. Törlés és visszaadás

A rendezvény adatait (telepítési kódok, leadek, logó, kitűzőfájlok) a rendezvény záró dátumát követő 90. napon automatikusan töröljük. Addig az Ügyfél az alkalmazásból exportálhatja adatait (CSV/XLSX). A szolgáltatás végén a Fluid Digital az Ügyfél választása szerint visszaadja vagy törli a személyes adatokat, legkésőbb 90 napon belül, kivéve, ha uniós vagy magyar jog a tárolásukat írja elő. Korábbi törlés kérhető az info@qrleadcapture.com címen.

11. Tájékoztatás és ellenőrzés

A Fluid Digital az Ügyfél rendelkezésére bocsát minden olyan információt, amely a GDPR 28. cikkének való megfelelés igazolásához szükséges, elsősorban jelen Szerződés, mellékletei és az Ügyfél kérdéseire adott írásbeli válaszok útján. Lehetővé teszi és elősegíti az Ügyfél vagy az általa megbízott, titoktartásra kötelezett ellenőr által végzett auditot, ideértve a helyszíni vizsgálatot is, legalább 30 nappal korábbi írásbeli bejelentés alapján, munkaidőben, a működés zavarása nélkül, rendszerint évente legfeljebb egyszer (kivéve felügyeleti hatósági előírás vagy incidens esetén), az Ügyfél költségére. A Google infrastruktúrájának ellenőrzését a Google független tanúsítványai és jelentései (pl. ISO/IEC 27001, 27017, 27018, SOC 2) biztosítják.

12. Felelősség és záró rendelkezések

A felek érintettekkel szembeni felelősségére a GDPR 82. cikke irányadó. A felek egymás közötti viszonyában – a jogszabályok által megengedett mértékben – az ÁSZF felelősségi szabályai alkalmazandók. Jelen Szerződésre a magyar jog irányadó; jogvita esetén az ÁSZF-ben megjelölt bíróság illetékes. Ha valamely rendelkezés érvénytelen, a többi rendelkezés hatályban marad. A magyar változat fordítás; eltérés esetén az angol változat az irányadó.

1. melléklet – Az adatkezelés részletei

Tárgy és jelleg	A QR Lead Capture mobilalkalmazás és adminisztrációs felületek tárhelyszolgáltatása és üzemeltetése: adatok gyűjtése (beolvasás, kézi rögzítés), tárolása, megjelenítése, exportálása és törlése.

Cél	Lehetővé tenni, hogy a kiállítók rendezvényeken leadeket gyűjtsenek és kezeljenek, a szervezők pedig kezeljék a kiállítókat és a telepítési kódokat.
Az érintettek kategóriái	Rendezvénylátogatók és más kapcsolatok, akiknek az adatait rögzítik (leadek); az alkalmazást használó kiállítói munkatársak; a szervezők által feltöltött kiállítói kapcsolattartók.
A személyes adatok típusai	Leadek: név, e-mail, telefonszám, cég, beosztás, cím, weboldal, közösségi profilok, jegyzet, kategória, egyedi mezők, rögzítés időpontja. Kiállítók: név, e-mail, cég, telepítési kód, eszköznevek, eszközök száma.
Különleges adatok	Nem cél. Az Ügyfél a szabad szöveges mezőkben nem rögzíthet különleges adatot (GDPR 9. cikk).
Gyakoriság	Folyamatos, a szolgáltatás időtartama alatt.
Megőrzés	A rendezvény záró dátumát követő 90. napig, vagy az Ügyfél utasítására korábbi törlésig.
Helyszín	Tárolás: Google Cloud EU (Belgium, Hollandia). Feldolgozás: EU, valamint a 3. mellékletben felsoroltak szerint az USA.

2. melléklet – Technikai és szervezési intézkedések

- **Titkosítás:** minden kapcsolat TLS-sel (HTTPS) titkosított; a tárolt adatokat a Google Cloud titkosítja (AES-256).
- **Hozzáférés – alkalmazás:** a felhasználók telepítési kóddal azonosítják magukat; az adatbázis biztonsági szabályai biztosítják, hogy minden kiállító csak a saját leadjeit olvashassa és írhasssa.
- **Hozzáférés – portálok:** a szervezői portálhoz csak az eseményhez rendelt e-mail-cím fér hozzá; a rendszeradminisztráció név szerint engedélyezett adminisztrátorokra korlátozott, jelszóval és kétlépcsős azonosítással (TOTP) védve.
- **Legkisebb jogosultság:** a szolgáltatásfiókok csak a szükséges jogosultságokkal rendelkeznek; a hozzáférési kulcsok nem a forráskódban vannak.
- **Elkülönítés:** az adatok rendezvényenként és kiállítónként logikailag elkülönülnek.

- **Adattakarékosság és törlés:** automatikus törlés a rendezvény záró dátuma után 90 nappal; csak a szolgáltatáshoz szükséges adatokat gyűjtjük.
- **Naplózás és felügyelet:** műszaki naplók a Google Cloud Loggingban (30 nap); hibafigyelés a Firebase Crashlytics-szel.
- **Infrastruktúra:** Google Cloud adatközpontok fizikai védelemmel, redundanciával és független tanúsítványokkal (ISO/IEC 27001, 27017, 27018, SOC 2).
- **Változáskezelés:** kódmódosítás verziókezelésen és átnézett pull requesteken keresztül; automatizált telepítés.
- **Személyi intézkedések:** titoktartási kötelezettség; hozzáférés csak az arra rászoruló munkatársaknak.
- **Incidenskezelés:** dokumentált incidenskezelési eljárás; az Ügyfél értesítése 48 órán belül (9. pont).

3. melléklet – További adatfeldolgozók

Adatfeldolgozó	Szolgáltatás	Helyszín	Továbbítási garancia
Csomós Róbert e.v. (4183 Kaba, Liget utca 8.)	A szolgáltatás fejlesztése és üzemeltetése; az alábbi Google Cloud szolgáltatásokat ő veszi igénybe	EU – Magyarország	–
Google Cloud EMEA Ltd. (Írország)	Tárhely, adatbázis (Cloud Firestore), fájl tárolás, háttérszolgáltatások, adminisztrációs felületek (Google Cloud / Firebase)	EU – Belgium, Hollandia, Lengyelország	–
Google LLC (USA)	Az alkalmazás bejelentkezési funkciója (kiolvassa a kiállító nevét és e-mail-címét, nem tárol); Firebase Authentication (globális szolgáltatás); Firebase Crashlytics hibajelentések (lead-adat nélkül)	USA / globális	EU–USA adatvédelmi keretrendszer; általános adatvédelmi kikötések (SCC)

Adatfeldolgozó	Szolgáltatás	Helyszín	Továbbítási garancia
Google Ireland Ltd. (Írország)	Céges e-mail (Google Workspace), ügyfélszolgálati kommunikációhoz	EU / globális	Általános adatvédelmi kikötések (SCC)

Utolsó frissítés: 2026. október 17.

Signatures • Aláírások

Only needed when the DPA is signed as a separate document. · Csak külön dokumentumként történő aláírás esetén szükséges.

Customer / Ügyfél

Company / Cég: _____

Name, title / Név, beosztás:

Place, date / Hely, dátum:

Signature / Aláírás

Fluid Digital Kft.

4400 Nyíregyháza, Könyves utca 2/a

Dávid Kukoly, CEO / Kukoly Dávid
Ügyvezető

Place, date / Hely, dátum:

Signature / Aláírás