GUIDE TO THE MOST FREQUENTLY USED PLATFORMS OF THE ON-LINE SPACE

With the advance of technology, the diverse services of the digital space have become part of our daily life (social networking, work, shopping, etc.).The opportunities offered by on-line platforms, however, also raise new issues as service providers not only have access to unprecedented amounts of data but can also combine them to create complex user profiles and social networks with unregulated and often untransparent security, purpose, processing and transfer. Therefore, the security of user data (data collection, securing the right to erasure, etc.) and the issue of advertisements/search results targeting users are particularly important.

This guide focuses on the most common platforms in Hungary such as Facebook (including its most popular products: Instagram, Messenger and WhatsApp) and Google (including its search engine, Google Maps, YouTube, Gmail, cloud-based data storage and data sharing, etc.).

TABLE OF CONTENTS

1. How can your personal data be misused?

Disclosing your personal data on an on-line platform carries a number of risks including identity theft, where unauthorised persons access your personal data or other confidential information and use it for purposes detrimental to you such as ordering goods and services on your behalf, taking out a loan in your name, etc.

Monitoring on-line user behaviour and activities also makes it possible to create personality profiles of users. According to the General Data Protection Regulation (hereinafter: GDPR) [1] profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. A study by the Hungarian Competition Authority[2] states it as a requirement that consumer information should clearly state how operators of digital comparison tools use user data for profiling and displaying targeted advertisements to finance the platform. It also points out that many consumers are not aware of the nature and value of the data they provide. As a result, in some cases, they mistakenly believe that a service can be used free of charge and without any risks or obligations. If, however, collecting data on consumer interests, behaviours and shopping habits and, in possession of such data, selling targeted advertising to business customers are an essential element of a site's business model, then the services provided by the site are not free of charge, as consumers pay for the service with their own data.

It should be emphasised, therefore, that it is primarily the user's i.e. your responsibility to make an informed decision about which personal data you wish to share on-line. You should be aware that by sharing your personal information publicly, your disclosed information may be used in a manner that is expressly not intended, or may have adverse consequences for you!

[1] Article 4 (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC

[2] The effects of digital comparison tools on consumer decisions, 2020 https://www.gvh.hu/pfile/file?path=/dontesek/agazati_vizsgalatok_piacelemzesek/piacelemzesek/piacelemzes_digitalis_osszehasonlito_eszkozok_tanulmany_2020_03_12&inline=true

2. What can you do to protect your personal data?

First of all, if you think you should share and disclose your personal data, limit the disclosure to the narrowest possible data categories. The sensitivity of the data (e.g. political opinion, religion or beliefs, health data, etc.) included in the individual data categories should also be taken into account.

As regards cookies (to be presented later in this guide), it should also be stressed that their acceptance requires your express consent in each case. Therefore, before agreeing to the use of cookies, always read the relevant privacy policy!

You should also pay proper attention to the content you publish when adjusting your privacy settings, so if possible, do not make your posts public, i.e. available to anyone; instead, limit them to your friends, for example, or only to yourself.

3. What are Facebook and Google products?

- **Facebook products** include Facebook, Messenger, Instagram, Portal branded devices, Bonfire, Facebook Mentions, Facebook Stores, Spark AR Studio, Audience Network, NPE Team apps and any other function, application, technology, software, product and service offered by Facebook Inc. or Facebook Ireland Limited.
- **Google products** include YouTube, Gmail, Chrome, Maps, Photos, Drive, Google Ads, and Analytics.

4. Who manages your personal data when you use these products?

The data manager of personal data is Facebook Ireland Ltd. and Google Ireland Ltd., multinational companies based in Ireland but owned by parent companies registered in the United States. Data processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, storage, alignment or combination and erasure.

5. What personal data are processed when using the above products?

Using Facebook[3] or Google[4] products entails **the processing** of an exceptionally large number and variety of **personal data.**

[3] Facebook Privacy Policy is available at https://en-hu.facebook.com/privacy/explanation
[4] Google Privacy Policy is available at https://policies.google.com/privacy?hl=en_US

When users register on the Facebook platform, they provide *public data*, such as name, sex, and user ID.

! IMPORTANT: remember that these public data about you will be visible to everyone!

However, you can customise your personal profile settings at your discretion, including by adding more personal data (such as date and place of birth, studies, place of work, etc.) that are not visible to all. In addition, sensitive data ("*special data*") such as religious affiliation or political opinion can also be shared with the world. You are free to decide whether you want to provide additional personal information; nobody is obliged to do so. The personal data you wish to share with the Facebook community can be set in the privacy settings of your profile. You may decide to share only *public data*, and no other personal information. You can also change your privacy settings so that anyone can see your personal information (even people you do not know), or you can limit the visibility of these data to your friends or a group of them.

! IMPORTANT: read Facebook's Privacy Policy before deciding on the personal data you want to publicly disclose about yourself!

Think of this as if you were telling your personal information to strangers in the street!

If you use a Facebook product for **your purchases or other financial transactions**, Facebook will have information on, among other things, your bankcard, shipping and contact details.

- To increase the usability of its products, Facebook collects the data of the persons with whom you come into contact while using the products (e.g. WhatsApp, Instagram).
- Both Facebook and Instagram monitor and record the **use of Facebook products**, i.e. what and how often users view, and what people, websites, groups and search tags (aka hashtags or #)[5] they are connected.

[5] Hashtags make it easy to find all the entries for a subject marked with #, similar to the index of a book.

When using Google products, users of a Google Account also provide personal information, such as their name, password, and even their phone number.

! IMPORTANT: always read Google's Privacy Policy!

- In addition to the personal information you voluntarily provide when using certain Google products, **data you would never think of**, such as your emails, photos, videos, IP addresses, numerous info-communication network data, location data, telephone numbers, text messages, list of telephone calls, shopping data, partner lists and browsing history as well as the websites you have visited, the applications on your device and your data traffic, etc. **may also be processed.** The data uploaded to Google's cloud services for backup and recovery purposes are also processed.
- Google consolidates processed data **collected from its various services and user devices**. Thus, if users access Google services from both their mobile phone and computer, these data can be consolidated in order to get an even more accurate picture of user habits. Like Facebook, Google also monitors and records the use of Google products.

6. For what purposes are your personal data processed?

Personal data are processed in order that they can be used for the highest possible number of purposes. Thus, Facebook and Google both collect various data to customise user experience, offer content, and display ads that may interest users (e.g. editing feeds, events of interest, recommending Facebook groups). In addition, based on the data collected **marketing materials** can also be displayed or sent to users who can also set their preferences in this regard and send feedback (e.g. "Already purchased it", "Why am I seeing this?", "Irrelevant content", or "Disturbing content"). Your personal data may also be processed for compliance and security purposes. Accordingly, "two-factor authentication" as a security measure requires users to provide a separate authentication code to confirm the login attempt when they try to access Facebook from a browser or mobile device that Facebook cannot identify. Such a primary security method could be a code received in a text message (SMS) or the use of an external authentication app (e.g. Google Authenticator, LastPass).

! IMPORTANT: both Facebook and Google are engaged in direct marketing activities, displaying selected ads based on the data and activities disclosed by users or the data collected with or without their consent or knowledge. These ads are displayed to users based on their activities related to the products and affiliates of these multinational companies as well as their partners, customers, and business partners.

Users' data provided in Facebook or Instagram profiles, as well as their location, favourite websites, logins, or, in the case of Google, search and watch history are all taken into account when future ads and feeds are created.

7. What rules do Facebook and Google follow in processing your personal data?

Given the wide variety of data processing operations performed by Facebook and Google, **various national and Community norms may apply** to the processing of your personal data, such as the GDPR and Act CXII of 2011 on the Right of Informational Self-Determination and on the Freedom of Information. In addition to the applicable laws, the Terms of Service of Facebook and Google provide a framework for lawful data processing.

Upon registration, you accept the Terms of Service of Facebook and Google, which also comprise their Privacy Policy. You enter into a contractual relationship with the service provider, so the legal basis for the processing of your personal data will primarily be the performance of the contract.

Depending on the services used, the legal basis for the processing of your personal data may also be:

- your consent,
- fulfilment of a legal obligation that Facebook or Google must meet.

8. How can you influence the ads displayed to you?

There are several ways to influence personal ads. These include customisation, disabling certain data services and data transmission functions, and setting search results.

Customisation: although Facebook and Instagram display various ads using your interests, attitude and relationships, you can also customise the ads that appear on Facebook.
Hiding/setting ads:

- You can **hide** a specific ad displayed on Facebook or Instagram, or all ads from an advertiser.
- In addition, **you can review and change your ad settings** to affect the ads that appear on Facebook. So, you can, for example, hide certain ad topics (alcohol, pets, etc.) for a certain period of time or permanently.

Disabling specific data: by disabling data on marital status, employer, job position, studies, etc. provided voluntarily on Facebook, users can stop receiving ads customised on the basis of these data.

Like Facebook, Google also enables the customization of privacy settings, even if you are signed out of your user account.

Search results: You can disable search activities in your browser from influencing search results. You can set *the type of Google ads that will appear* and decide on whether your browser-specific *YouTube search and watch history* influence your use of YouTube.[6]

9. What are "cookies"?

Cookies are small text files that websites store with the express consent of users on the computer or mobile device that they use for visiting their pages. You may encounter different types of cookies in the on-line space. For instance, some cookies allow information (e.g. language settings) related to your previous website visits to be stored, others can identify users, or are necessary for the provision of full services.[7] Note that if you do not wish to give your consent to the use of the latter type of cookies, the service may not function comprehensively or properly on your IT device, because service providers often make full user experience conditional upon the acceptance of these cookies. You should know what cookies you accept, what type of data they provide and to whom, and what apps can access, process, or transfer them.

10. Where to turn to if you want to file a complaint or report an infringement in relation to the processing of your personal data by Facebook or Google?

The European headquarters of Facebook and Google are in Ireland. The 'primary supervisory authority' under the General Data Protection Regulation (the supervisory authority with

[6] Setting Google ads: https://support.google.com/accounts/answer/2662856?p=adssettings_activity&hl=hu&visit_id=637274817779308499-3126507607&rd=1

[7] Information about display resolution or accessing webpages via mobile devices or a computer

competence over the data controller's or the data processor's place of central operations or single place of business) is **the Irish Data Protection Commission** (DPC).

In Hungary it is the **National Authority for Data Protection and Freedom of Information** (hereinafter: the NAIH, customer service: +36 (1) 391-1400 and ugyfelszolgalat@naih.hu) in its capacity as an autonomous government body that performs the tasks and exercises the powers related to the processing of personal data of the independent supervisory authority as defined in the GDPR. Although the primary supervisory authority is located in Ireland, you can always contact the NAIH if you wish to file a complaint in connection with the processing of your personal data or think that your rights have been violated.

- The NAIH may address complaints related to the processing of personal data filed with it, or take action if the GDPR is likely to have been breached provided that such complaints or breaches have a significant impact only in Hungary and they concern only one place of business of Facebook or Google in Hungary.
- If such a case, the NAIH immediately informs the primary supervisory authority in Ireland, which will then decide whether to take action, considering whether the controller or the processor has an establishment in Hungary. **The NAIH may only proceed with the prior consent of the Irish supervisory authority**.

11. How to complain if you think Facebook or Google is engaged in unfair commercial practices against you as a consumer?

If you think that Facebook or Google is engaged in unfair commercial practices[8] against consumers, you can report the case or submit a complaint to the **Hungarian Competition Authority** (customer service: +36 1 472-8851 and ugyfelszolgalat@gvh.hu).

12. What content can you post on your Facebook platform?

If you violate the Terms of Service of Facebook Inc., it may restrict your use or access to the website.

[8] A commercial practice shall be unfair if it fails to meet the standard of the special skill and care which a person carrying out that commercial practice may reasonably be expected to exercise, commensurate with the fundamental principle of good faith and fairness, and it appreciably reduces or is likely to appreciably reduce the possibility for the consumer to whom it is directed, whom it reaches or to whom it is addressed to make an informed decision with regard to the goods, based on the necessary information, and thereby causes the consumer or is likely to cause him to take a transactional decision that he would not have taken otherwise (Article 3(2) of Act XLVII of 2008 on the Prohibition of Unfair Commercial Practices against Consumers).

Based on the "*community principles*" of Facebook, for example, content that incites or promotes serious violence may not be published. All users must refrain from, among other things:

- acts of hate speech,
- content that glorifies violence or celebrates the suffering or humiliation of others,
- cruel and insensitive content, and
- posting of content harmful to minors.

! IMPORTANT: Facebook as operator may restrict or remove content that violates the Community Principles by means of their own content moderation, without the prior permission, approval (or knowledge) of the administrator of the given Facebook page.

Administrators of Facebook pages or any Facebook user, **including you may report to Facebook** any content that violates the Community Principles.

Like Facebook, Google also requires you to use its services in full compliance with its Terms of Service, including, but not limited to, the fact that Google reserves the right to remove some or all of the content that aids and abets child pornography, trafficking in human beings or harassment or violates someone else's intellectual property.

13. What remedies are at your disposal against a decision to remove content posted on Facebook?

In respect of certain specific content (nudity, pornography, hate speech, and violent content), you may request Facebook to review its decision. Facebook (using a support message folder) notifies you in a message of the removal of the content you posted. If Facebook allows a review of this posted content, you may initiate a review by means of submitting a "Request of review".

14. What is the "Oversight Board" and what will it exactly do?

Facebook's Oversight Board is an independent and autonomous committee that will function **as a forum for redress against Facebook's decisions on removing certain content**. The Board will have 40 members who will serve a fixed term of three years and can be re-elected

for up to three terms. The Board will focus on hate speech, harassment, and people's rights to privacy and personal safety and security.

! IMPORTANT: the Oversight Board is independent of national governments, including the government of Ireland, as well as the US administration. It is a body similar to international arbitration courts whose decisions cannot be challenged for the time being.

If, in your opinion, your content has been removed from the digital platform unlawfully or without a cause, you can, in certain cases, file an appeal with the independent Oversight Board within 15 days. If the Board changes Facebook's decision, **its decision will be binding on Facebook**, which will have to comply with the decision within 7 days, unless, for example, the content violates copyright or local law. Users involved in the individual cases may express their views on the matter at hand in writing to the Board. Facebook does not rule out the possibility of board members' hearing users at a later date either. The most complex and controversial matters may also be referred to the Board by Facebook itself. In such cases, the members of the Board will decide whether to address such matters.

Each issue or case will be assessed by a panel with rotating membership. Panel decisions will be reviewed by the full Board before finalization. If the majority disagrees with the panel's findings, however, another panel will be appointed to re-assess the case. A selection committee in which Board members rotate every 3 months, will determine the issues to be addressed by the Board. The selection committee will consider aspects such as whether an issue potentially affects many users, whether it is essential to the continuation of public discussions, or whether it raises questions related to Facebook's policies. The Board will have up to 90 days to decide on such issues.

Facebook may also request general guidance from the Board on certain matters. However, such guidance will not be binding on Facebook. Facebook may also request the Board to express opinion or draw up guidelines.