11 November 2020

# Final Decision

**Complaint against [redacted] – Personal Data Breach (Articles 33 and 34 GDPR), Security of Processing (Article 32 GDPR)**

IMI A56ID: 64211
IMI Case: 72377
IMI A61VMN: 151854
IMI A60DD: 156281

The Hessian Commissioner for Data Protection and Freedom of Information (hereinafter "HBDI") refers to the complaint lodged by Mr. [redacted]. (hereinafter "Complainant") against [redacted] (hereinafter "[redacted]") with the Dutch Data Protection Authority concerning a possible security breach in the authorization process of [redacted] servers.

## 1. Case description

The Complainant has reported a possible security breach in the authorization process of certain [redacted] servers through the ethical Hacker program "HackerOne".

According to the Complainant, the personal data that could be reached through the breach were for example friend lists.

[redacted] has replied to the Complainant that this incident was a known issue and that they are implementing measures.

On 23 September 2020, the Dutch Data Protection Authority informed the HBDI that the Complainant considers the problem solved and wishes to withdraw his complaint.

## 2. Investigation outcome

HBDI contacted [redacted] in July 2019. In its answer, [redacted] confirmed that a possible security breach had been reported through the platform "HackerOne".

[redacted] has explained that in the underlying HackerOne Report a point of attack was described, which concerned so-called matchmaking servers of the older [redacted] generation of the [redacted] and the [redacted] [redacted]. These are servers that are used to carry out matchmaking for games of the above-mentioned [redacted] platforms with online multiplayer function, in which players are assigned other



Gustav-Stresemann-Ring 1 · 65189 Wiesbaden · Telephone +49 6 11 14 08 – 0 · Fax +49 06 11 14 08 – 9 00 (or – 9 01)
Email poststelle@datenschutz.hessen.de · Web www.datenschutz.hessen.de

players to the online game according to criteria defined by the system and internal rankings/leaderboards are calculated for the participating players. For each individual game title with corresponding functionality, there is a separate matchmaking server. The matchmaking servers are created in the system architecture as logical servers.

To be distinguished from the matchmaking servers and not the object of the reported attack are the actual account servers. On these account servers, if created by the user, the user account - on the [redacted] in question this is the [redacted] - is administered, which contains the information deposited by the user when registering the [redacted], such as the email address or other data required for the identification of the user.

Due to the limited functionality of a matchmaking server, it contains only very limited data. This is mainly technical information necessary for matchmaking, such as region/time zone and skill level to be able to assign adequate opponents to the players, as well as dynamic IP addresses of players currently in matchmaking to enable the establishment of a peer-to-peer connection between them. The dynamic IP address itself is not stored in the matchmaking server.

In addition, the users and friends connected to the users (referred to as friend lists in the complaint) are assigned internal identification numbers on the matchmaking server which do not allow third parties to identify the players themselves and do not contain contact information of the users, contrary to what is claimed in the complaint.

A further functionality of a matchmaking server is the mapping of in-game (visible to other players) rankings/leaderboards of players involved in an online multiplayer mode. Furthermore, if supported by the respective game title, scores achieved by the user in the game, game scenes saved by the user (so-called replay data), a public mail in the game or, for example, the items of clothing selected for a game character can be stored on the servers.

The general procedure in case of reported possible points of attack, which was also used in the present case, initially provides for a comprehensive technical analysis. One measure taken is the development of appropriate patches to close the point of attack. In addition, the package of measures can provide for the shutdown of individual affected servers in individual cases. For servers where patching requires less technical effort, the detected attack points are closed first.

As a direct result of the report, [redacted] conducted a comprehensive analysis of the named point of attack and discovered the weakness in user authentication described in the report on older matchmaking servers of the aforementioned older[redacted] platforms. As a result of this analysis and taking into account the relevance and user activity on affected matchmaking servers, [redacted] started to close the attack point and to patch affected servers according to the previously mentioned criteria in order to protect the servers from corresponding hacker attacks. The matchmaking server for the



Gustav-Stresemann-Ring 1 · 65189 Wiesbaden · Telephone +49 6 11 14 08 – 0 · Fax +49 06 11 14 08 – 9 00 (or – 9 01)
Email poststelle@datenschutz.hessen.de · Web www.datenschutz.hessen.de

game [redacted] named in the report was already patched in December 2016. The incident was also investigated with [redacted]'s external data protection officer.

A manipulation of the matchmaking servers could not be detected during the analysis.

The point of attack depicted in the report concerns exclusively older matchmaking servers of game titles for the [redacted] and [redacted] of the [redacted]. These are both older models, many of which have not been produced or distributed by [redacted] for years, and game titles that generally have low user activity. As correctly described in the complaint, the matchmaking servers for game titles of the current [redacted] generation of the [redacted] are not affected.

In [redacted]'s opinion, the described facts do not constitute a notifiable violation of the protection of personal data pursuant to Article 33 or 34 GDPR.

The data stored on the matchmaking servers is primarily technical data which [redacted] can link internally with a user account and thus subjectively allow [redacted] to identify the user. [redacted] does not request any clear names via the existing account systems which are not the subject of the attack and does not use selected user names (so-called nicknames). According to the user agreements, which the user agrees to, user names may not contain any clear names. For a third party, however, the necessary personal reference is missing because a third party cannot identify the persons behind the users with the data on the matchmaking servers. This is especially true for dynamic IP addresses which are only available in real time and are not stored in the matchmaking Server. Third parties lack the legal and factual means to identify a natural person behind the user. At most, at the time the connection is established, it is possible to roughly determine the regional dial-in node of the user with whom the hacker exploiting the point of attack is initiating a matchmaking process. However, this may differ considerably from the actual location of the person. A general "reading" of all online players connected via the matchmaking server and their assigned dynamic IP addresses, which must be shared between the users in order to establish the peer-to-peer connection, was not possible via this point of attack.

Moreover, access to the matchmaking servers concerned is not possible without further ado, but requires advanced hacking capabilities.

Nevertheless, [redacted] states to take the security of their servers very seriously and has therefore taken the steps described above.

[redacted] is of the opinion that even on the assumption of a personal data breach, an unauthorized break-in into the server using the corresponding criminal energy and access to the data stored there would in all probability not lead to a risk to the rights and freedoms of natural persons. The data concerned is not data with which an attacker could cause harm to a data subject, e.g. through identity theft, let alone identify a person.



Gustav-Stresemann-Ring 1 · 65189 Wiesbaden · Telephone +49 6 11 14 08 – 0 · Fax +49 06 11 14 08 – 9 00 (or – 9 01)
Email poststelle@datenschutz.hessen.de · Web www.datenschutz.hessen.de

## 3. Decision

In the course of the investigation, the HBDI has found that the reported incident does not constitute a personal data breach within the meaning of Articles 33, 34 GDPR since personal data of [redacted] users is not concerned. The incident had only minor impacts (without data protection impact) and has been adequately resolved.

The Complainant also considers the problem solved and has withdrawn the complaint.

In its Draft Decision of 13 October 2010 the HBDI has informed the supervisory authorities concerned accordingly. No objections to the Draft Decision were raised.

The HBDI therefore concludes the proceedings with this Final Decision.

The Hessian DPA



Gustav-Stresemann-Ring 1 · 65189 Wiesbaden · Telephone +49 6 11 14 08 – 0 · Fax +49 06 11 14 08 – 9 00 (or – 9 01)
Email poststelle@datenschutz.hessen.de · Web www.datenschutz.hessen.de