Insufficient encryption in self-service solution by the police

Date: 07-04-2021

Decision

Public authorities

The Danish Data Protection Agency expresses criticism of the National Police after having examined a self-service solution for applying for a weapons permit on its own initiative, because the solution did not support a sufficient degree of encryption.

Journal number: 2020-432-0049

Summary

In a case of self-operation, the Danish Data Protection Agency examined the police's self-service solution for applying for firearms permits.

It was found that the then ASP solution only supported TLS version 1.0. The National Police stated that this version was the highest that the solution in question supported and that work was being done to replace it.

The Danish Data Protection Agency is of the opinion that forms and web solutions for handling personal data place demands on security, in particular that you, as the data controller, ensure that personal data does not come to the attention of unauthorized persons. Information of a nature worthy of protection, including information on social security numbers, must therefore be secured in a way where the content cannot be accessed by unauthorized persons.

This can be done by encrypting the transport layer (TLS) in version 1.2 or higher. Furthermore, the Danish Data Protection Agency is of the opinion that TLS versions 1.0 and 1.1 contain known vulnerabilities that do not ensure the necessary confidentiality and integrity of the information exchanged.

The decision should be seen as a general reminder that it is not an expression of appropriate security if the technologies used to ensure confidentiality and integrity (in this case TLS) contain known weaknesses and where there are readily available secure standards. In addition, the Authority is of the opinion that the support for the phased-out versions of TLS in question must be switched off in both e-mail and web solutions.

Decision

The Danish Data Protection Agency hereby returns to the case, which the audit initiated on its own initiative after becoming aware that by accessing the website www.digimeld.politi.dk/vaaben/HTML/index.aspx?type=p70401, where you can apply on a

weapons permit, is warned that the site uses weak encryption and that unauthorized persons have the opportunity to access the information entered. In connection with the application, you must e.g. enter his social security number.

By letter of 4 November 2020, the Danish Data Protection Agency requested the National Police for an opinion in the case, after which the National Police issued a statement on 26 November 2020.

Decision

Following a review of the case, the Danish Data Protection Agency finds grounds for expressing criticism that the National Police's processing of personal data has not taken place in accordance with the rules in Article 32 (1) of the Data Protection Regulation [1]. 1.

Below is a more detailed review of the case and a justification for the Danish Data Protection Agency's decision.

2. The opinion of the National Police

The National Police has stated that the weapons application system on the police website consists of a web application form and an e-mail sending function, respectively. In connection with entering personal information in the application form, the connection between the police server and the applicant's browser is protected with TLS 1.0 encryption until the entry is completed. When the entry of information in the application form is completed, the information is sent via the e-mail sending function to an e-mail address at the Police Administrative Center (PAC), which processes the actual application for a firearms permit. When the submission is completed, the form will close down, after which all entered information as well as any attachments will be deleted from the police server and the weapon application system. Emails from the self-service solution are sent via a VPN solution that uses AES256 bit encryption.

The Danish National Police has further stated that TLS version 1.0 encryption is used in the web application form on the website for applying for a firearms permit, while end-to-end encryption is used in the mail sending function. The reason why TLS 1.0 encryption is used in the web application form is that TLS 1.0 is the highest level of encryption that can be run on the existing solution. However, the National Police is aware of the Danish Data Protection Agency's recommendation on the use of TLS 1.2 or newer for encryption on the transpost layer. The National Police is i.a. therefore in the process of implementing a new application solution for weapons licenses, where a stronger encryption is used, so that the weapons application system becomes even more secure.

The National Police has finally stated that the National Police has initiated the development of a new weapons application

system based on the Danish Business Authority's form engine, which uses the current TLS version at the time of implementation, which is expected to be TLS 1.3. The National Police expects that the new application solution will be commissioned in the first quarter of 2021.

Justification for the Danish Data Protection Agency's decision

It is clear from Article 32 (1) of the Data Protection Regulation 1, that the data controller must implement appropriate technical and organizational measures to ensure a level of security appropriate to the risks to the rights and freedoms of natural persons.

It is the Data Inspectorate's opinion that the handling of personal data worthy of protection places greater demands on security, including ensuring that the data controller does not make personal data known to unauthorized persons. Information of a nature worthy of protection, including information on social security numbers, must therefore be secured in a way where the content cannot be accessed by unauthorized persons. This can be ensured by encryption on the transport layer (TLS) in version 1.2 or higher. Furthermore, the Danish Data Protection Agency is of the opinion that TLS version 1.0 contains known vulnerabilities that do not ensure the necessary confidentiality and integrity of the information exchanged.

Based on this, the Danish Data Protection Agency finds that the National Police - by using TLS version 1.0 encryption in the web application form on the website for applying for a firearms permit - has not had appropriate technical measures to ensure an appropriate level of security, cf. 1.

On the basis of this, the Danish Data Protection Agency finds that there are grounds for expressing criticism that the National Police's processing of personal data has not taken place in accordance with the rules in Article 32 (1) of the Data Protection Ordinance. 1.

The Danish Data Protection Agency has noted that the National Police has changed the solution for applying for a firearms permit, and that the National Police is now using a new firearms permit system based on the Danish Business Authority's form engine.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46 / EC (General data protection regulation).