SME-related activities of the Hungarian Data Protection Authority



National Authority for Data Protection
and Freedom of Information

Dr. Julia Sziklay

Vice President of the Hungarian Data Protection Authority

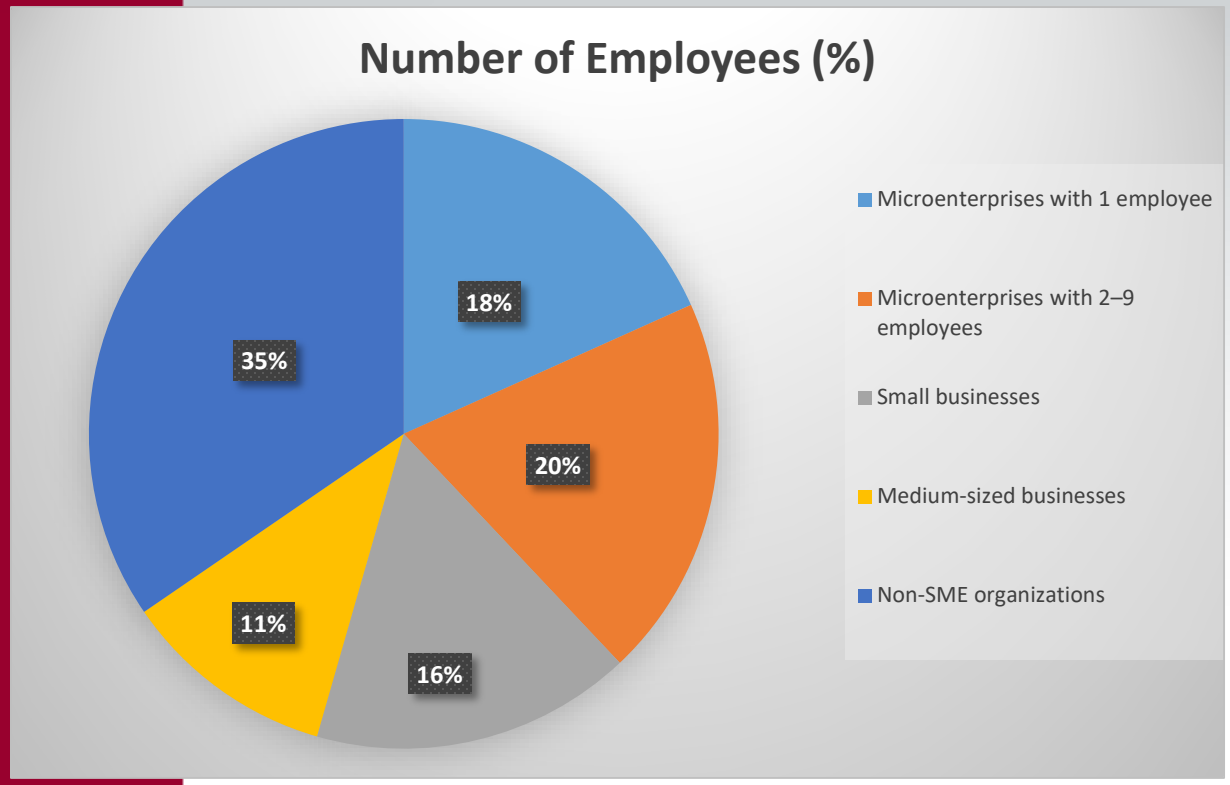
AWARE Project Coordinator

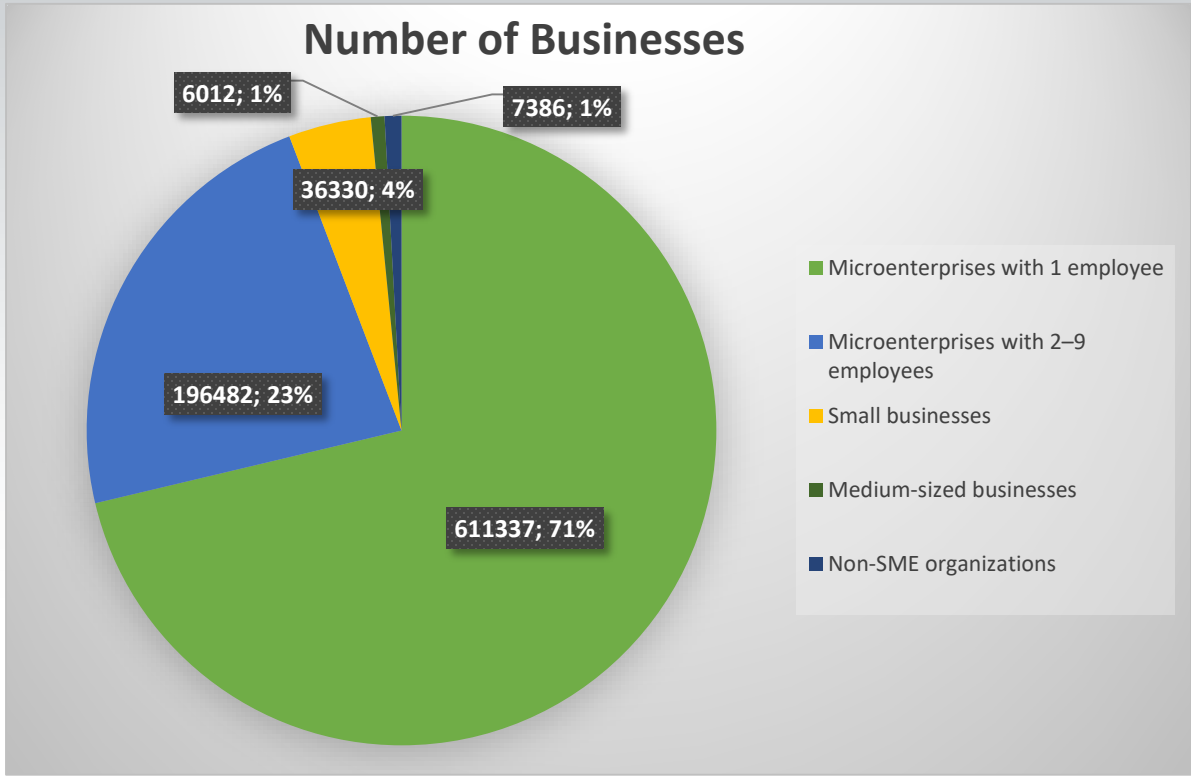
4 November 2026

National Authority for Data Protection and Freedom of Information

Background of the project - The role of SMEs in Hungary

AWARE 2025-2026



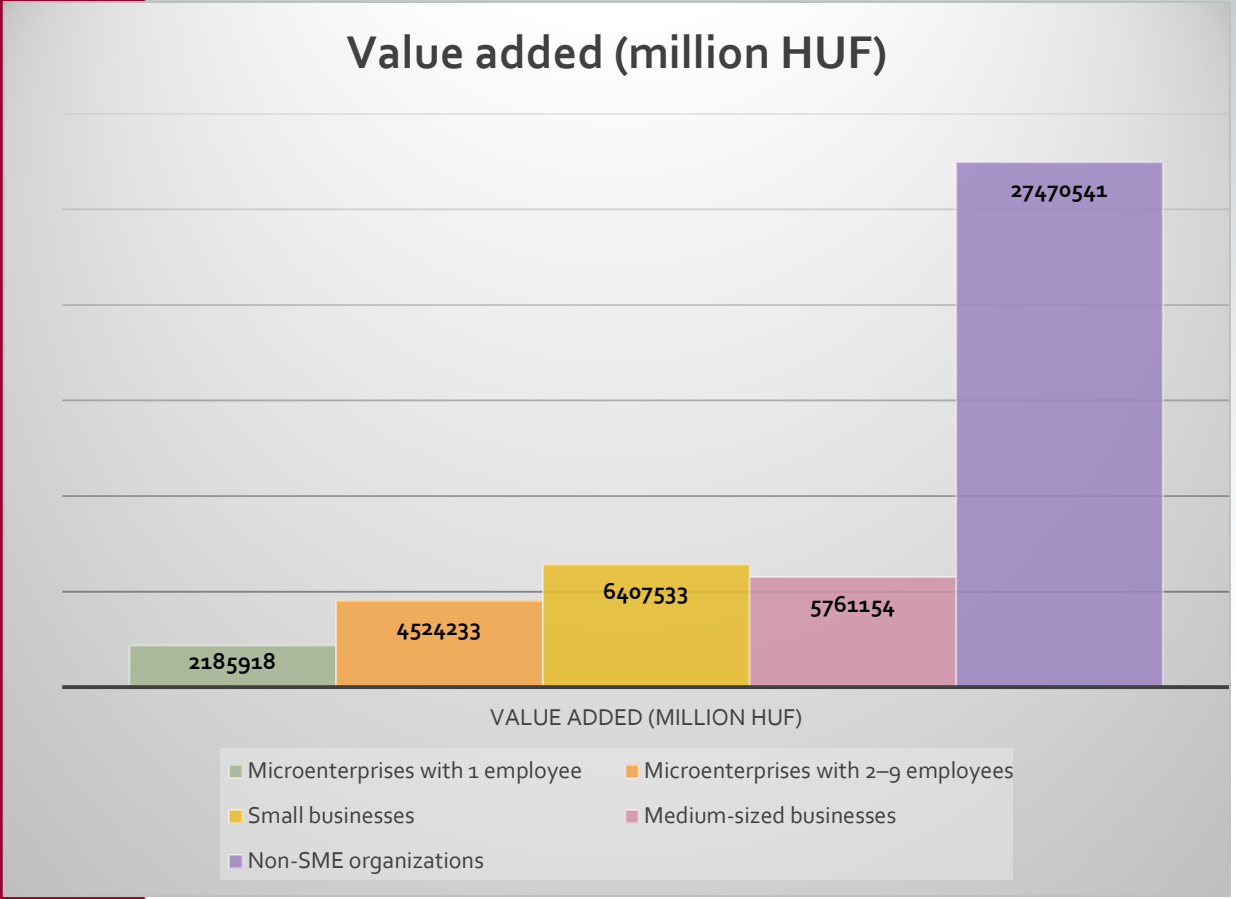


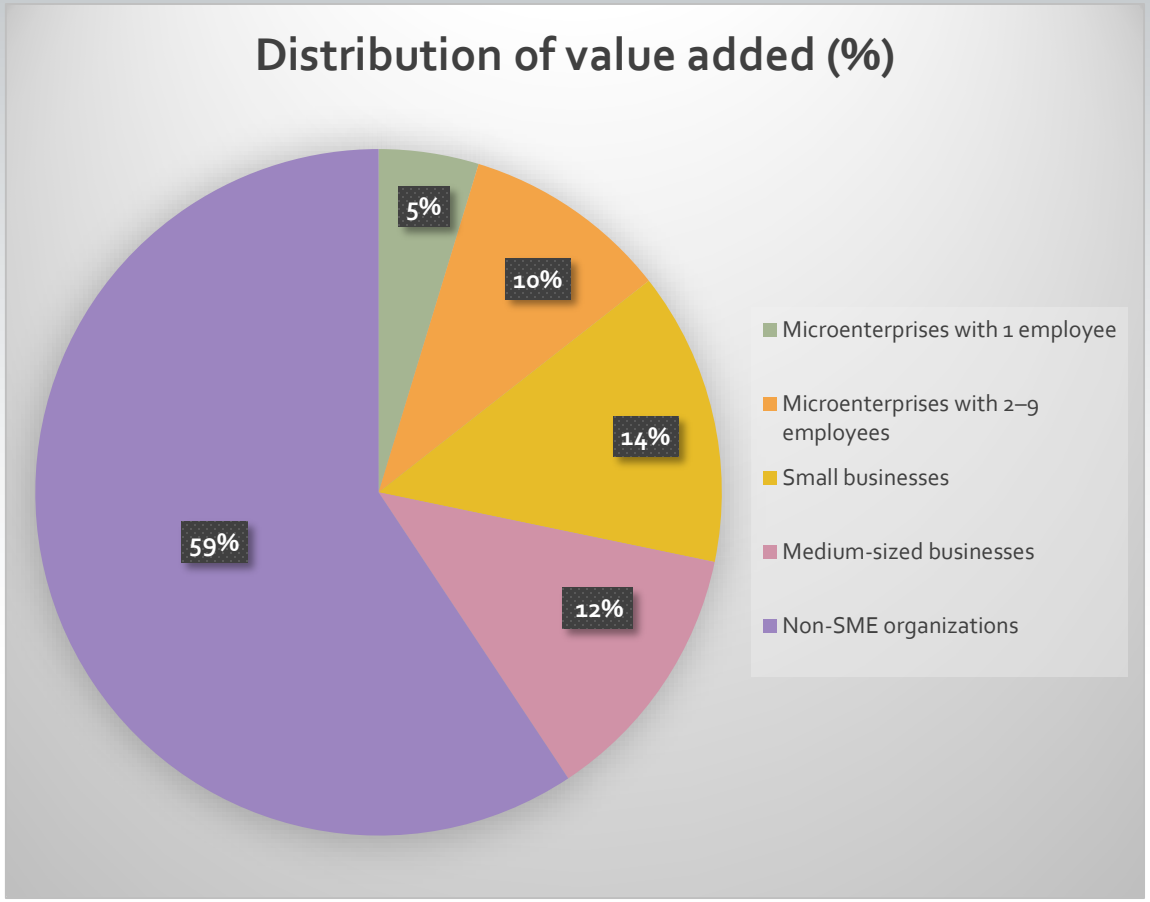
Source: Central Statistical Office (2024)

National Authority for Data Protection and Freedom of Information

Background of the project - The role of SMEs in Hungary

AWARE 2025-2026





Source: Central Statistical Office (2024)

National Authority for Data Protection and Freedom of Information

Background of the project - STAR II Project - Overview

AWARE 2025-2026

BENEFICIARY	National Authority for Data Protection and Freedom of Information (NAIH)
CONSORTIUM PARTNERS	Vrije Universiteit Brussel Trilateral Research Ltd.
PROJECT NAME	SupporT small And medium enterprises on the data protection Reform II
PROJECT ACRONYM	STAR II
PROJECT NUMBER	814775
TOTAL BUDGET	EUR 560 580
AMOUNT OF EU FUNDING	EUR 448 544
TIME PERIOD	1 August 2018 – 31 December 2020

National Authority for Data Protection and Freedom of Information

STAR II Project
Aims and results

AWARE 2025-2026

- Reviewed DPA awareness-raising activities and analysed SMEs' experience within first months of the functioning of the GDPR.
- Ran an awareness raising campaign for SMEs and operated a trial **information hotline** (for 12 months) to respond to SMEs' questions, measuring its performance and the most frequently asked questions.
  https://naih.hu/files/KKV-hotline-GyIK.pdf
- On that basis – prepared a **digital guidance for DPAs** on good practices in running a hotline and raising SME awareness.
- Published an innovative, **FAQ-based handbook** (digital and printed) for SMEs on EU personal data protection law.

National Authority for Data Protection and Freedom of Information

STAR II Project Results

AWARE 2025-2026

Handbook prepared for SMEs

https://naih.hu/files/handbook_the_gdpr_made_simpler_for%20smes_eng.pdf



EDITED BY
LINA JASMONTAITĖ-ZANIEWICZ
ALESSANDRA CALVI
RENÁTA NAGY
DAVID BARNARD-WILLS

THE GDPR
MADE SIMPLE(R) FOR SMEs

GPRC Guaranteed Peer Reviewed Content www.gprc.be
The GPRC label (Guaranteed Peer Review Content) was developed by the Flemish organization Boek.be and is assigned to publications which are in compliance with the academic standards required by the VABB (Vlaams Academisch Bibliografisch Bestand).

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

The content of this publication represents the views of the editors only and is their sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This work is licensed under the Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported License.
To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-sa/3.0/
DOI: 10.46944/9789461171092

Open Access
Publishing in European Networks

Book design: Frisco.be

© 2021 VUBPRESS
VUBPRESS is an imprint of ASP nv (Academic and Scientific Publishers)
Keizerslaan 34, 1000 Brussels
Tel. +32 (0)2 289 26 56
Fax +32 (0)2 289 26 59
Email: info@aspeditions.be
www.vubpress.be

ISBN 978 94 6117 069 9 (print)
ISBN 978 94 6117 109 2 (ePDF)
ISBN 978 94 6117 110 8 (epub)
NUR 820, 980
Legal deposit D/2021/11.161/026

National Authority for Data Protection and Freedom of Information

STAR II Project Handbook

AWARE 2025-2026

Contents

Acknowledgements 9
Liability and legal disclaimer 10
List of abbreviations 11

Preface 13

Introduction 17
Background 17
Structure 18
Method 20
Bringing in added value 21
Target audience 21

1. Navigating support 23
1.1. National and regional Data Protection Authorities (DPAs) 24
1.2. The European Data Protection Board (EDPB) 26
1.3. The European Data Protection Supervisor (EDPS) 27
1.4. The European Union Agency for Cybersecurity (ENISA) 28
1.5. The European Union Agency for Fundamental Rights (FRA) 28
1.6. The EU funded initiatives 29
1.7. The International Association of Privacy Professionals (IAPP) 30

2. Personal data protection basics 31
2.1. What is personal data and its processing? 31
2.2. What are the possible roles for an SME in the processing operations? 41
2.3. What are the principles applicable to the processing of personal data? 49
2.4. What are the possible legal bases for personal data processing? 51
2.4.1. Background 51
2.4.2. How to choose among different legal bases? 52
Consent 52
Contractual relationship 56
Compliance with a legal obligation 57
Vital interests of data subjects or of another person 58
Public interest or exercise of an official authority vested in the data controller 58
Legitimate interests pursued by the data controller 59
2.5. What are the data subjects' rights? 62
2.5.1. Background 62
2.5.2. What are data subjects' requests, and how can these be fulfilled? 64
Right to transparency and information 64
Right to access 66
Right to rectification 69
Right to erasure, a.k.a. right to be forgotten (right to de-listing) 69
Right to restriction of processing 71
Right to data portability 72
Right to object 73
Right to not be subject to a decision based solely on automated decision-making (or profiling) 74
2.6. The obligation to appoint a Data Protection Officer (DPO) 75
2.6.1. Background 75
2.6.2. Is the appointment of a DPO mandatory for SMEs? 75
2.6.3. Who should be a DPO? 79
2.6.4. What tasks can be assigned to a DPO working for an SME? 80
2.6.5. Can an SME share a DPO with other organizations? 83
2.6.6. What should be considered before appointing a DPO? 83

3. The theory and practice of a risk-based approach 85
3.1. Background 85
3.2. What is a risk in the GDPR? 86
3.3. What does cause risks? 87
3.4. How can risks under the GDPR be evaluated? 89
3.5. What are the provisions embedding a risk-based approach in the GDPR? 95
3.6. How can a risk-based approach benefit SMEs? 96
3.7. A risk-based approach in practice 97
3.7.1. Responsibility of the controller and the principle of accountability 97
Background 97
What does an SME need to do to be accountable? 98
What are the other examples of accountability measures? 99
What are the advantages of accountability for an SME? 100
3.7.2. Data protection by design and data protection by default 101
Background 101
What does data protection by design entail? 102
How to evaluate the appropriateness and effectiveness of data protection by design measures? 105
What does data protection by default entail? 107
What are some examples of measures implementing data protection by default? 107
3.7.3. Records of processing activities and other documentation 110
Background 110
What does documentation require? 110
What are the other types of documentation required by the GDPR? 114
3.7.4. Security of processing 116
Background 116
How is the security obligation related to other provisions? 116
What organizational security measures can an SME take? 117
What technical security measures can an SME take? 118
What level of security is required? 119
3.7.5. Personal data breach notification 120
Background 120
Under what conditions is a notification to the DPA required? 122
What documentation could help an SME to prepare for a data breach? 123
Under what conditions is a notification to affected individuals required? 124
3.7.6. Data protection impact assessment (DPIA) and prior consultation 128
Background 128
Who has to perform a DPIA? 129
When is a DPIA mandatory? 130
When is a DPIA not required? 135
When is a new (revised) DPIA required? 136
How should a DPIA be conducted? 137
3.7.7. Codes of conduct 144
Background 144
What are the advantages of codes of conduct? 146
How to select the appropriate code of conduct? 146
3.7.8. Certification 147
Background 147
What are the advantages of certifications for SMEs? 148
How should you choose between different certifications? 149

4. SMEs and employees' data 151
4.1. What are the possible legal bases for processing the personal data of employees? 152
4.2. When and what monitoring activities are permissible? 154

Annex I – National laws 157

About the editors 169

National Authority for Data Protection and Freedom of Information

Our current project: AWARE Overview

AWARE 2025-2026

In February 2025 the NAIH has launched a new EU data protection project to map and increase GDPR awareness among micro-enterprises, with a particular focus on the **beauty industry and the private healthcare sector**.

BENEFICIARY:	Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH)
CONSORTIUM PARTNER:	Trilateral Research Limited
PROJECT NAME:	Raising GDPR AWAREness for micro-enterprises, with specific attention paid to the beauty industry and private healthcare sector.
PROJECT ACRONYM:	AWARE
PROJECT NUMBER:	101193182
TOTAL BUDGET:	EUR 277.779
AMOUNT OF EU FUNDING:	EUR 250 000
FUNDING RATE (%):	90%
PLANNED COMPLETION DATE:	31 January 2027

Aims of the project

- The AWARE project runs from 1 February 2025 to 31 January 2027 and is part of the CERV-2024-DATA programme of the European Commission.

- The project is being implemented under the supervision of **NAIH** in consortium with **Trilateral Research Ltd**, an Irish research and development company specializing in new technologies and data protection issues.

- The overall aim of the project is to provide education tailored to the needs of SMEs.

Aims of the project

- AWARE emphasises the rights of data subjects, in particular the importance of the right of access, and facilitating compliance with obligations arising from data subject requests through innovative tools.
- The project pays particular attention to employment issues and the mapping of information society services.
- It gives priority to the personal data protection of women and children.

Target groups

- Focus on Hungarian micro-SMEs operating in the beauty industry and private healthcare sector.
- Target groups were selected with due care, taking into account the fact that both the cosmetics industry and private healthcare are constantly growing sectors.
- Cooperation with Hungarian and EU SME organisations and chambers of commerce is of particular importance.

In focus

- Data subject rights
- Video surveillance
- Processing of personal data of minors and women
- Operation of websites or social media accounts
- Use of online payment and appointment booking platforms
- Artificial intelligence applications



National Authority for Data Protection and Freedom of Information

Outputs completed to date

AWARE 2025-2026

Informative project website in English and Hungarian

https://naih.eu/in-english



Outputs completed to date

Repository of useful links

Consists of 100 items of useful links, online tools, guidance documents, research projects with the results achieved or still ongoing, e.g. **Driven by Risk** project:

No.	Title	Link	Source	Language(s)	Country of issuance (if applicable)	Brief description	Date	Keyword 1	Keyword 2	Keyword 3	Keyword 4	Output (for research projects only)
89	byRisk - Driven by risk: Fostering data protection risk assessment for SMEs and raising risk awareness among the general public	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-details/43251589/101193352/CERV?isExactMatch=true&frameworkProgramme=43251589&topicAbbreviation=CERV-2024-DATA&order=DESC&pageNumber=1&pageSize=50&sortBy=title	European Project	English	Greece	byRisk pursues two strategic goals: i) to facilitate SMEs to properly identify and analyse all the data protection and privacy risks occurring in their data processing operations, and ii) to raise awareness regarding data protection and privacy risks to a vast spectrum of stakeholders, including SMEs and the general public. To this end, byRisk will develop a a Risk Assessment Tool, that will provide the means for the identification and analysis of data protection and privacy risks in an intuitive manner, leveraging context-aware questionnaires; as well as a Risk Awareness Tool, targeting the general public, in order to foster data subjects' awareness of data protection and privacy risks through appropriate visualisations of the risks, the associated harms, as well as precautions and countermeasures.	2025-2027	SMEs	Personal data	Processing	Security of processing	Ongoing project

National Authority for Data Protection and Freedom of Information

Outputs completed to date

AWARE 2025-2026

Brochure – Beauty industry

Real-life situations



„I would like to take photographs both before and after my client's treatment. We would like to publish the images on our social media platforms and on our website to show the results that can be achieved with our treatments. What do I need to keep in mind to ensure full compliance with data protection regulations?"

„…photographs taken in connection with the provision of the service do not automatically become „property" of the service provider in the sense that the service provider could dispose of them without restrictions or use them freely. With regard to the personal data appearing in the photographs, the data subject continues to have the right to self-determination. Therefore, any use of the images for purposes not necessary for the provision of the service – in particular their publication for marketing purposes or as reference material – must be based on an appropriate legal basis for data processing, which in practice usually means the data subject's prior, voluntary, specific, informed and unambiguous consent."

Outputs completed to date

Brochure – Private healthcare sector

Real-life situations



„During the first consultation, the patient mistyped a letter in their email address on the registration form, resulting in the electronic invoice and the medical report being sent to the wrong person. As a healthcare provider, is there anything I need to do about this? Am I liable for the consequences? I sent the documents to the email address provided by the patient."

„In this case, sending the documents to the wrong address still constitutes a personal data breach, regardless of whether the incorrect email address was provided due to an error on the part of the patient. This is because the controller's liability extends not only to their own fault, but also to any event that results in personal data becoming accessible to an unauthorised person. …"
."

Outputs completed to date

- Slides for stakeholders
- Podcast interview with the Vice President of NAIH
- Radio campaign
- Detailed interviews with the target groups (see next slide)

National Authority for Data Protection and Freedom of Information

Key findings of interviews and EU survey

AWARE 2025-2026

In-person interviews and EU survey conducted with Hungarian micro-SMEs.

Private healthcare sector:

A higher level of data protection awareness can be observed, due to stricter legislation and the sensitive nature of health data. The majority of businesses

- are aware that they process special categories of personal data,
- have a privacy notice,
- apply some form of formal data security measures,
- recognise the importance of data protection responsibilities.

Beauty industry:

Several of these businesses

- do not accurately identify what personal data they process,
- do not have adequate documentation or privacy notices,
- apply informal data security measures.

GDPR viewed as a "necessary administrative burden" rather than a conscious data protection framework.

National Authority for Data Protection
and Freedom of Information

AWARE
2025-2026

Thank you for your attention!

AWARE project:
https://naih.eu/in-english

Nemzeti
Adatvédelmi és
Információszabadság
Hatóság

TRILATERAL
RESEARCH
Innovation
& Research

Funded by
the European Union

Funded by the European Union, under grant no. 101193182. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.