Report Data breaches 2023

Report April 2024

AUTORITEIT
PERSOONSGEGEVENS

Preface

The digital society is developing rapidly. Data is playing an increasingly important role in people's lives. The increasing use of data offers opportunities, but also brings risks. Risks such as data breaches.

In 2023, the Dutch Data Protection Authority (Autoriteit Persoonsgegevens or AP) received more than 25,000 reports from companies, governments and other organisations in relation to data breaches. Personal information was unintentionally shared with others and ended up in the public domain or was stolen. The latter is often the work of hacker gangs and other cybercriminals, for whom personal data is worth money. These cyberattacks have a major impact on victims whose personal data has been breached, as well as on the affected organisation.

Cyberattackers often target IT suppliers. They manage more and more data on behalf of companies or government agencies. These organisations remain responsible for the careful processing of data of their customers and citizens.

The AP recognises that organisations affected by a cyberattack often underestimate the risk to victims. As a consequence they do not always inform the victims. While this is often necessary – and mandatory. A so-called victim notification can help people to be more alert to phishing messages.

The AP monitors this and takes action. Last year for example, after a major cyberattack on IT supplier Nebu, the AP intervened at 34 Nebu customer organisations that underestimated the risks of this data breach and wrongfully did not inform people about the inicident. After intervention by the AP they corrected this.

People must be able to trust that organisations handle their personal data securely. This trust forms the foundation for the exchange of data that is necessary for services and business operations in the Netherlands. Data breaches damage this trust. All this means that the protection of personal data is an ongoing challenge for all of us.

The AP advocates a society in which people have control over their personal data and in which organisations are intrinsically motivated to properly protect the personal data they process. A society in which the digital resilience of people and organisations is growing. With the realisation that this will only work if we do this together.

Aleid Wolfsen
Chairman of AP

Table of Contents

1. Summary

Many victims due to cyberattacks

In 2023, a total of 25,694 data breaches were reported to the AP. Based on the reports of these data breaches, the AP can estimate the number of individuals affected by cyberattacks in the past year to be approximately 20 million. This concerns individuals in the Netherlands as well as in other countries (within and outside Europe).

Read more on page 11 →

Cyberattack at Nebu

In March 2023, a cyberattack took place at Nebu, an IT supplier of software for market and customer satisfaction research. The AP estimates that this data breach affected 2.5 million individuals. After the data breach, the AP strictly monitored compliance with the reporting obligation to victims in order to strengthen their digital resilience.

Read more on page 7 →

Victims of cyberattacks often not informed due to risk being assessed too low

Data breaches due to cyberattacks generally pose high risks for victims, such as financial damage or identity fraud. In 2023, more than 7,000 people reported identity fraud to the Central Identity Fraud Reporting Centre (CMI). Supervision by the AP is partly aimed at helping affected organisations make a correct risk assessment.

Read more on page 5 →

Collaboration is crucial

Affected organisations making a correct risk assessment is a first step towards a digitally resilient society. Insight into facts and figures about data breach reports can help achieve this. That is why the AP makes information from data breach reports available to the Dutch Central Statistical Office for scientific research. Furthermore, the AP is preparing to collaborate more intensively with other cybersecurity regulators on the NIS2 Directive. The NIS2 Directive sets strict requirements for the cybersecurity of Dutch vital infrastructure, such as government and hospitals.

Read more on page 10 →

2. Risk of cyberattacks underestimated

A brief overview

- On average, 69% of organisations affected by a cyberattack estimate the risk for victims to be too low. On average, 46% of organisations inform victims. This is evident from an analysis performed by the AP.
- People who don't know they have fallen victim to a data breach, may be caught off guard by a phishing attack or fall victim to scams or identity fraud.
- Organisations are practically always obliged to report data breaches due to cyberattacks to the AP and to the victims.

Victims of cyberattacks often not informed

The AP has analysed the risk assessment of organisations that have reported a cyberattack. The AP looked at cyber-attacks involving datasets containing sensitive personal data. The results of the analysis are shown in the table on the right.

These data breaches involve, for example, medical data, credit card details or copies of passports. But also data breaches that apparently involve less sensitive personal data, such as email addresses, name and address details. Even these less sensitive kinds of data can be used by criminals for phishing messages.

What is a cyberattack?

In a cyberattack, criminals try to break into digital systems. For example, criminals can break into email accounts and send phishing e-mails to contacts. Other such examples are ransomware attacks in which criminals encrypt data, as a result of which the affected organisation can no longer access the data. In exchange for a ransom, criminals promise to provide the 'key' so that the organisation can access the data again.

RISK - ASSESSMENT BY ORGANISATIONS IN CYBER ATTACKS

Cyber attack involving:	% risk assessment: low	% risk assessment: high	% of individuals affected informed	Number of data breach reports in this category
special personal data	66%	34%	38%	198
copies of passports	67%	33%	60%	135
credit card details	70%	30%	59%	37
data of vulnerable indiviuals	68%	32%	53%	146
large number of e-mail addresses or telephone numbers	81%	19%	60%	96
Average:	**69%**	**31%**	**46%**	

Cyberattacks must practically always be reported to the AP and the victims

Data breaches due to cyberattacks generally pose high risks to victims, such as identity fraud, phishing or scams.

- With a stolen ID, criminals can commit identity fraud. For example, they can abuse the ID by taking out a loan in the victim's name.
- With name and contact details, criminals have sufficient information to create a credible phishing message. With an email or text message, criminals, while posing as the affected organisation, will try to steal money or information, such as login details.
- Credit card details allow criminals to make purchases.
- Usernames and passwords allow criminals to break into the user accounts of consumers.
- Stolen personal data can be added to existing datasets, which for example are for sale on the dark web. This data will ultimately be used in large-scale hacks, the goal of which is to gain access to user accounts.

That's why these types of data breaches must almost always be reported to the AP and the victims.

Low risk assessment is worrying

The AP concludes that too often individuals are wrongfully not informed in the event of a data breach due to a cyberattack. In many cases, cyberattacks pose a high risk to the victims in which sensitive personal data or data of vulnerable individuals are compromised. However, organisations that reported such cyberattacks in 2023 only estimated the risk to victims as high in 30 to 34% of cases.

This low percentage worries the AP. Too low a risk assessment can result in organisations deciding not to inform victims, or not informing them fully, and/or taking insufficient measures to prevent new data breaches. The AP takes measures to ensure that organisations correctly assess the risks to victims and take the required follow-up steps to control these risks.

EXAMPLES WHY ORGANISATIONS DO NOT INFORM VICTIMS

What wrong decision was made by many organisations in the Nebu data breach?	What is the right decision after a many cyberattack?
"We will not inform the victims of the data breach because it is unclear which data has been stolen." "We do not want to cause unnecessary unrest among victims."	If, after an investigation, you cannot rule out that the personal data to which the hacker had access to was (also) copied by the hacker, you must assume the worst-case scenario.
"The ransomware attack only concerned contact details, the risk is low. So we are not going to inform the victims."	Have large amounts of customers' contact details been captured by a hacker, such as e-mail addresses or telephone numbers, with additional personal data, such as name and address details? Or can this not be ruled out? In that case, you must inform the victims.

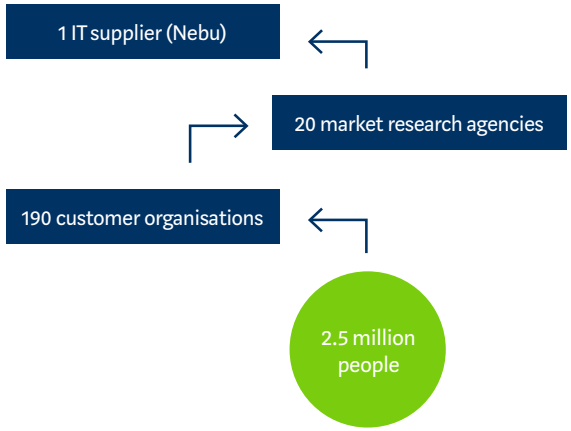
3. Cyberattack Nebu

A brief overview

- In March 2023, the servers of the Canadian company Nebu, an IT supplier, were hit by a cyberattack. This also affected organisations that were customers of Nebu.
- About 2.5 million Dutch individuals fell victim to the cyberattack.
- Organisations were obliged to inform victims because their email addresses, telephone numbers, name and address details had been compromised. Not all organisations did this because they estimated the risk for the victims as being too low.
- The AP targeted 34 customer organisations with interventions, as they failed to comply with their legal obligation to report to the AP and/or the victims.
- After intervention by the AP, a total of 50,000 victims were informed about the cyberattack.

Affected Dutch organisations

Nebu supplies software for market and customer satisfaction research to 20 market research agencies in the Netherlands. Various Dutch customer organisations, including VodafoneZiggo, use the services of these market research agencies. These Dutch customer organisations were obliged to report the data breach to the AP and the victims. They processed personal data of people who participated in a market or customer satisfaction survey. In most cases these were email addresses, telephone numbers, names and home addresses.



Data Protection Officer of VodafoneZiggo: “Practice how to deal with a data breach”

”Because the hack took place in Nebu’s systems, it was not immediately clear whether any customer data had been compromised and, if so, which ones. We immediately put together a team in case of these types of incidents. The team completes a pre-established process. We submitted a data breach report to the AP on time because it involved a hack. We also thought it was important to quickly inform our customers despite the fact that not all details of the hack were known yet. Some customers contacted us about this. Our customer service has played an important role in addressing our customers’ concerns. Conducting a ‘data breach exercise’ helps. This is useful for small companies, as they probably never have had to deal with a major breach before. For large companies it’s also useful, as they can practice how the different departments work together.”

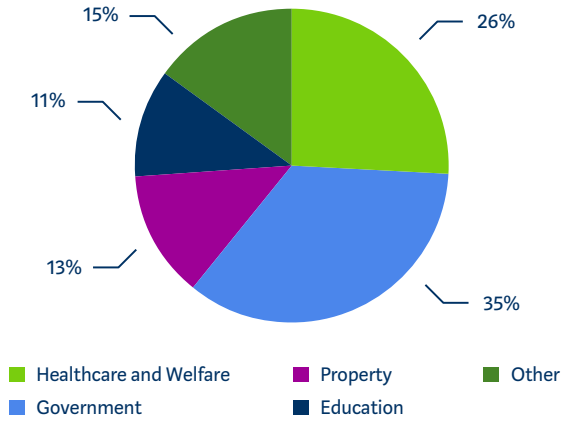
Supervision by the AP

Immediately after the data breach, the AP published a press release and called on affected organisations to comply with their reporting obligation, thereby ensuring that customer organisations immediately report the data breach to the AP and the victims. A large majority (82%) complied with the reporting obligation. The other 34 customer organisations only met their reporting obligations after intervention by the AP.

As a result of this intervention by the AP, approximately an extra 50,000 individuals were informed that they had fallen victim to the cyberattack. As a result, they are now extra alert to possible phishing messages. All 190 customer organisations ultimately fulfilled their reporting obligations. The AP is currently also conducting an investigation into IT supplier Nebu.

Customer organisations remain responsible for the proper processing of personal data at all times, even if the processing is outsourced to another organisation, such as an IT supplier.

SECTORS IN WHICH THE AP INTERVENED TO REMIND ORGANISATIONS OF THEIR OBLIGATION TO REPORT



Stichting Amsta informed its clients by text message

This foundation is one of the organisations affected by the cyberattack at Nebu. Stichting Amsta is a healthcare institution for Amsterdam residents who need complex, intense care. The data breach concerned names and telephone numbers of several clients and mainly of contact persons of clients. Stichting Amsta reported this data breach to the AP and informed those involved via a news report on their website. The AP then requested Stichting Amsta to personally inform those affected by personal letter. Stichting Amsta thought this approach was disproportionate. Amsta and the AP jointly thought about a feasible approach that was practical for Amsta and acceptable to the AP. Stichting Amsta then proposed to refer those affected to the news item on the website by means of a mass text message and, if necessary, to also speak to those affected afterwards. Stichting Amsta was thus able to personally inform all those affected with a relatively small effort, by using the contact details they had on record.

Data Protection Officer of La Providence: “Elderly people are extra vulnerable in the event of a data breach”

La Providence is a small-scale nursing and healthcare institution in Limburg. ”The data breach involved names and telephone numbers of our residents. A telephone number doesn’t seem sensitive. But after contacting the AP, we realised that informing the residents was the right thing to do due to their increased vulnerability to telephone scams by criminals. We were concerned that we would cause unrest if we were to inform the residents. We therefore adapted the report’s wording to the target group. We, for example, explained what a hack is. And we explained in the report how our residents can avoid scams by telephone or via WhatsApp. Next time we would like to inform our residents even faster. We will do this with a pre-established process and a template report to victims.”

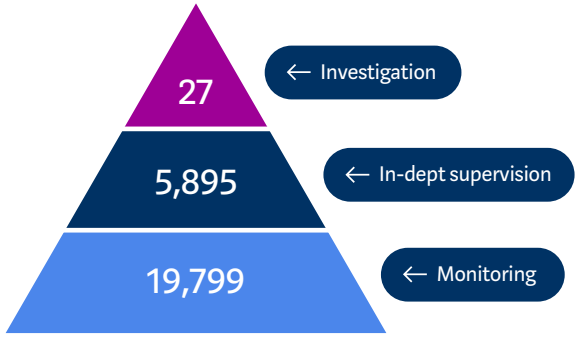
4. Risk-driven supervision AP

A brief overview

- The AP strengthens the digital resilience of people, companies and governments through supervision.
- In 2023, the AP took action in nearly 6,000 data breach reports.

Strengthening digital resilience
The supervision of the data breach reporting obligation is risk-driven and aims to strengthen the digital resilience of individuals, companies and organisations. The AP focuses on data breaches that pose the greatest risks for those affected and the protection of their personal data. Examples of this include data breaches as a result of cyberattacks, data breaches that affect large groups of individuals and data breaches involving special or sensitive personal data.

RISK-DRIVEN SUPERVISION

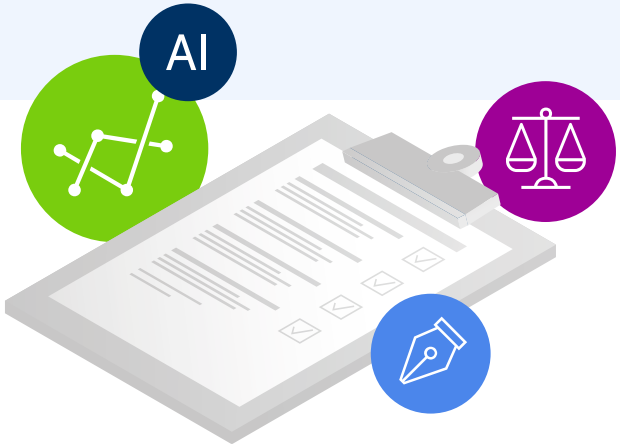


Monitoring
In 2023, a total of 25,694 data breaches were reported to the AP. In a large proportion of data breach reports, the AP takes no further action after an initial assessment. The AP received almost 20,000 of such data breaches in 2023. This involved, for example, data breaches due to incorrectly addressed post or emails.

In-depth supervision
Last year, the AP undertook additional supervisory efforts in 5,895 data breach reports. This was necessary because the AP identified major risks in these data breach reports. For example, because it involved many victims or (high volumes of) sensitive personal data. When receiving such reports, the AP carries out a more in-depth investigation.

Investigating
In 2023, the AP launched an investigation into 27 data breaches. According to the AP, these 27 data breaches posed the greatest risks to the victims. These mainly involved situations in which an organisation did not inform the victims of a cyberattack, while they were obliged to do so. And situations in which an organisation had taken insufficient new security measures to prevent new data breaches.

An investigation can be targeted at a single organisation, but also at a group of organisations. For example, during the investigation into the cyberattack at Nebu, the AP had to focus on several (customer) organisations.



5. Policy and regulations

A brief overview

- Under the NIS2 Directive, the AP works together with other regulators more intensively.
- The AP makes information from data breach reports available through the CSO.

Collaboration NIS2 Directive

The AP works together with other regulators to strengthen digital resilience. Under the NIS2 Directive, this collaboration will be further intensified. For example, NIS2 regulators will inform the AP of (potential) data breaches that organisations are obliged to report to the AP. Examples include cyber incidents that jeopardise business continuity, and which an organisation could have prevented by taking appropriate technical, operational and organisational measures.

The AP will work with NIS2 regulators to strengthen digital resilience in vital sectors. The EU has determined that the AP's power to impose fines takes precedence over that of other regulators if it concerns a data breach involving personal data.

Information from data breaches available through CSO

In 2023, the AP started a project together with the Dutch Central Statistical Office (CSO) to make information from data breaches reported to the AP available for scientific and statistical research in the secure microdata environment of the CSO. Research institutions can use this information for scientific research. The results can contribute to the resilience of organisations against cyber incidents. This is the first time that the AP has made information about data breach reports available in this way. The information cannot be traced back to individual organisations that have submitted a data breach notification.

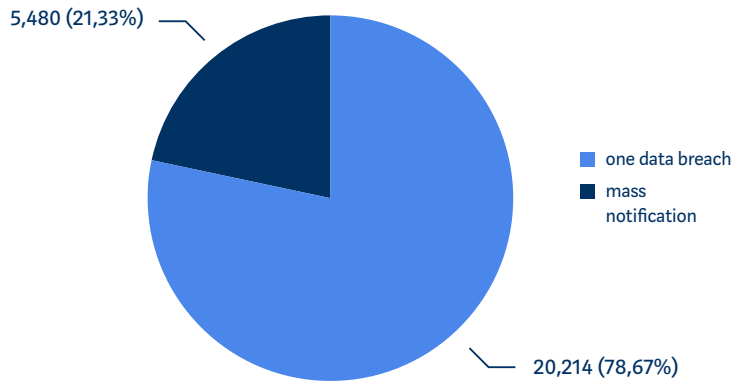
Through this project, the AP implements the advice of the Cyber Security Council: 'Making data breach reports available for research purposes'.

The first research file with reporting data will be published in the CSO catalogue around June 2024. From that moment on, authorised research institutions can submit a project application to the CSO.

6. Facts and figures

25.694 data breaches reported in 2023

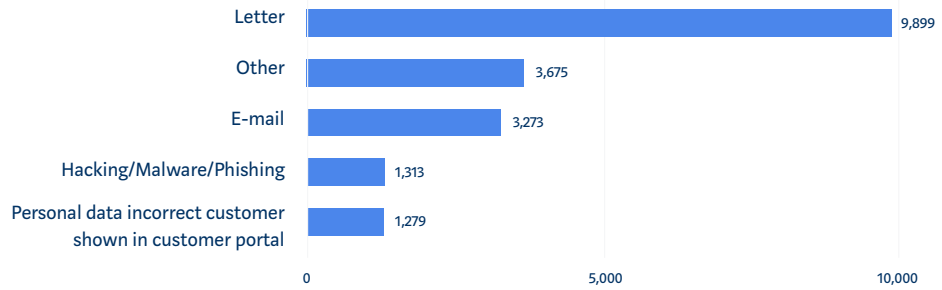
NUMBER OF DATA BREACHES IN 2023



In 2023, a total of 25,694 data breaches were reported to the AP. Of these, 5,480 data breaches were reported via a so-called mass notification. In a mass notification, an organisation reports multiple data breaches caused by incorrect mail dispatch. Mass reporting of similar data breaches can reduce the administrative burden for organisations.

Wrongly addressed letters reported most often

MOST REPORTED CATEGORIES OF DATA BREACHES - TOP 5



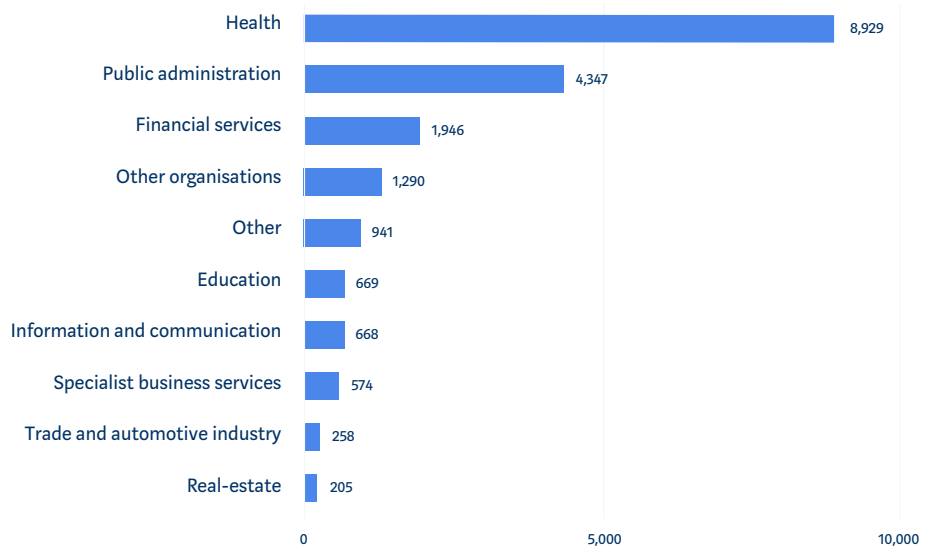
In 2023, as in previous years, most reports the AP received concerned incorrectly addressed letters containing personal data (9,899 reports). This type of data breach must only be reported to the AP in the event of a serious breach of privacy.

Reports in the category 'other' concerned the following types of data breaches:

- other (79.6%), for example: access by an authorised person, but without a valid reason, or: more personal data forwarded than necessary;
- personal data accidentally published (11.6%);
- network folder or location configured incorrectly (7.2%);
- personal data temporarily unavailable due to disruption (0.9%);
- documents with personal data discarded as waste paper (0.6%).

In 2023, most data breaches were reported by the health sector

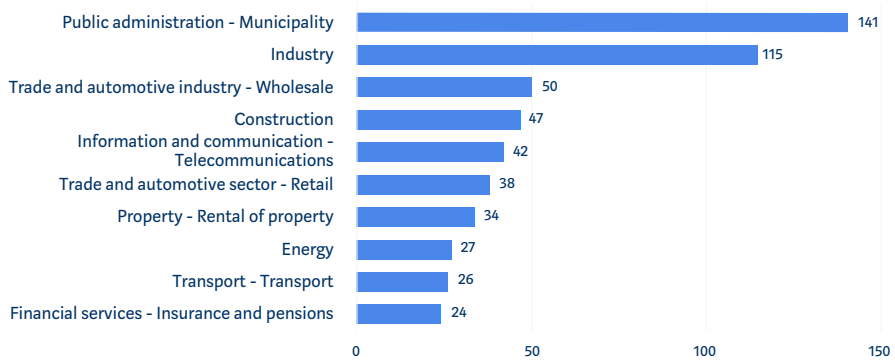
NUMBER OF REPORTS PER CAPITA IN SECTOR - TOP 10



In 2023, the AP received most data breach reports from organisations in the health sector (8,929), public administration (4,347) and financial services (1,946). Reports from the health sector concerned 5,779 cases of incorrectly addressed letters (65% of the total number of reports in the sector). In public administration this number was 2,218 (51% of the total number of reports in the sector), in financial services it was 881 (45% of the total number of reports in the sector).

Municipalities reported most cyberattacks

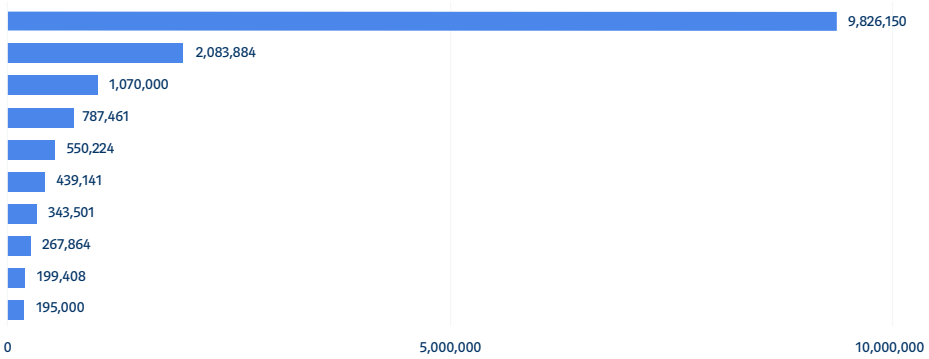
NUMBERS OF CYBERATTACKS PER SUB-SECTOR - TOP 10



The sub-sectors reporting most cyberattacks in 2023 were municipalities (141 reports), followed by organisations from the industrial sector (115 reports) and organisations from the trade and automotive sector - wholesale (50 reports).

Nearly 10 million victims due to largest cyberattack

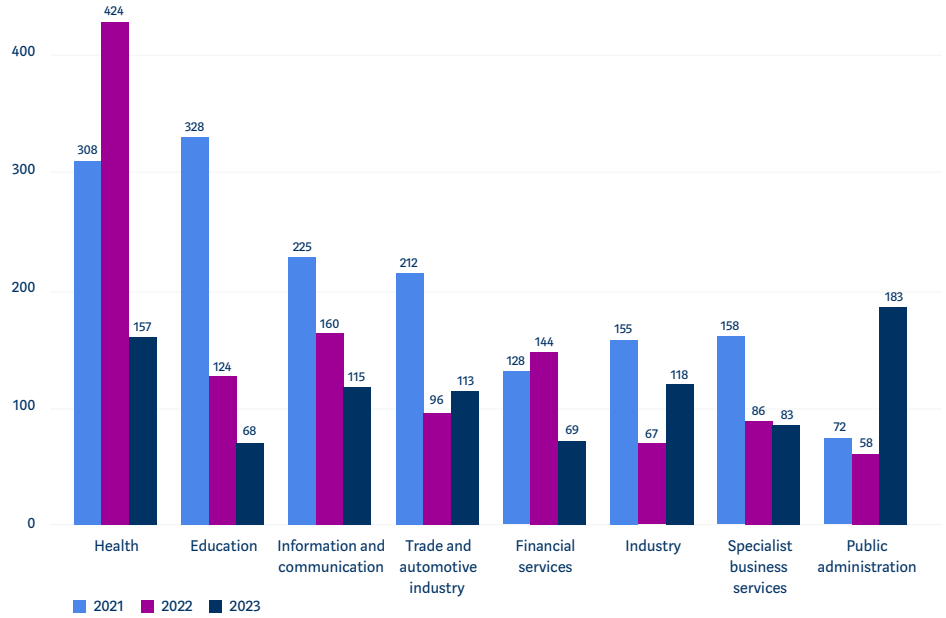
LARGEST CYBERATTACKS (IN NUMBER OF VICTIMS) - TOP 10



In 2023, AP received 1,309 data breach reports about cyberattacks, affecting a total of approximately 20 million people. The 10 largest cyberattacks affected a total of almost 16 million individuals (82% of the total number of victims).

In 2023, public administration reported most cyberattacks

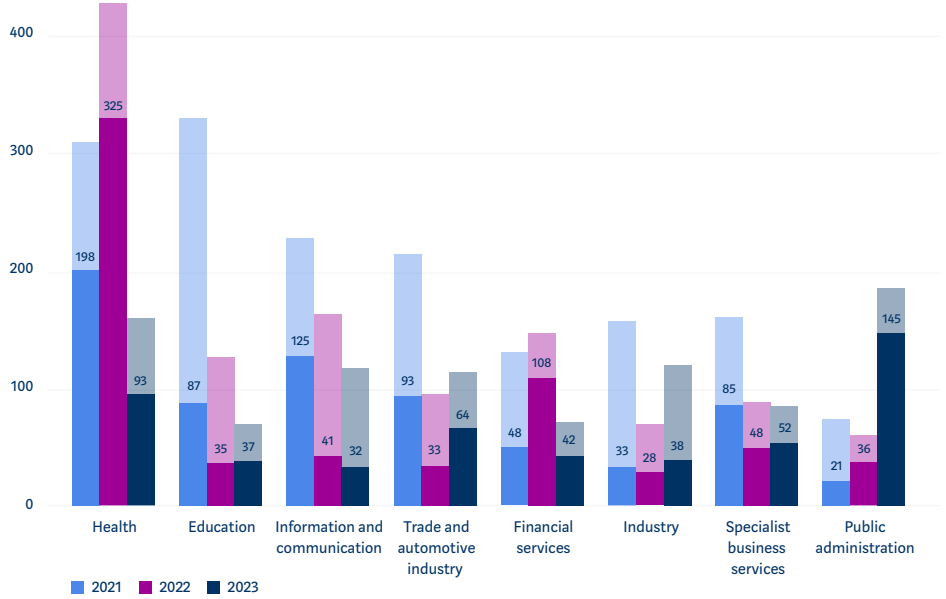
NUMBER OF CYBERATTACK REPORTS PER SECTOR IN 2021, 2022 AND 2023 - TOP 8



Number of reports following cyberattacks (hacking, phishing or malware incidents) fell to 1,309 reports in 2023, compared to 1,825 in 2022. In 2023, most cyberattack reports were made by organisations in public administration (183 reports), health (175 reports) and industry (118 reports). This is a shift from 2021 and 2022, when most reports of cyberattacks originated from education (2021) and health (2022).

In 2023, public administration reported most cyberattacks involving multiple organisations

NUMBER OF CYBERATTACK REPORTS PER SECTOR IN 2021, 2022 AND 2023 - TOP 8 - BREAKDOWN BY INVOLVEMENT OF MULTIPLE ORGANISATIONS



The table above lists the number of cyberattack reports involving multiple organisations. Especially the public administration and health sectors experienced frequent involvement of multiple organisations in a cyberattack. In many cases this involved cyberattacks at third-party companies (processors) such as IT suppliers, as a result of which multiple organisations were affected by the same data breach. In public administration, 145 of the 183 reports of cyberattacks involved third-party companies, or 79%. In the health sector, 93 of the 157 reports concerned cyberattacks, or 59%.

AUTORITEIT
PERSOONSGEGEVENS