CSR Cyber Security Raad

Visiting address
Turfmarkt 147
2511 DP The Hague

Postal address
PO Box 20011
2500 EA The Hague

I www.cybersecurityraad.nl
T +31 (0)70 751 5333 (secretariat)
E info@cybersecurityraad.nl

Minister of Justice and Security
Prof. F.B.J. Grapperhaus, LLM

Date
4 November 2020

Subject
CSR Recommendation
'Data breach reporting obligation'

Your Excellency,

The Cyber Security Council (CSR) is a national and independent strategic advisory body to the government and, through the government, to the business community with regard to matters of cybersecurity in the Netherlands. The council has 18 highly-placed representatives in public, private and scientific organisations. This unique composition allows the council to evaluate national and strategic cybersecurity challenges from multiple angles and issue well-considered strategic advice to the government and the business community. The council also monitors potential economic opportunities cybersecurity could offer our country.

The council would like to bring the following issue to your attention:

An obligation to report data breaches has been in effect in the Netherlands since 1 January 2016. Since the General Data Protection Regulation (GDPR) entered into force on 25 May 2018, the entire European Union has had a uniform set of laws and regulations concerning data protection in place, including a data breach reporting obligation. In the Netherlands, as a consequence, organisations are required to report all data breaches to the Dutch Data Protection Authority (Dutch DPA).

Each year, the obligation to report data breaches generates a substantial quantity of data in connection with security incidents involving personal data. Further analysis of these data may yield recommendations for improving our information security. The Dutch DPA is prepared to make these data available – under certain conditions, of course – for research purposes. The council and the Dutch DPA have, in close consultation, arrived at the opinion that a project should be carried out in order to determine the value of making these data available for research purposes. The project proposal drawn up in consultation has been appended to this letter as **Annex 1.**

Rationale

The recommendation to make data breach notifications available to researchers is in keeping with the report by the Netherlands Scientific Council for Government Policy (WRR) published in September 2019 under the

title ‘Preparing for digital disruption’[1]. This report calls for more widespread sharing of incident data, including notifications of data breaches submitted to and stored by the Dutch DPA.

The recommendation is also in line with a study that was conducted at the CSR's behest and which resulted in the report entitled ‘Scientific research data breach notification obligation’[2]. The importance of expanding access to data breach notifications is highlighted in the resulting report. This study was carried out by Erasmus University and Delft University of Technology at the behest of the CSR.

Contributing to increased digital resilience by deriving added value from reporting data

Information on data breaches is an important source of insight into the actual effects of security measures (or a lack thereof). Better research into the effects of such breaches enables organisations to take better decisions as to the security measures in which they should invest. This in turn may increase demand for cyber insurance, allowing insurers to mandate a higher basic level of security measures as part of their policy terms.

The council views information exchange as vital in order to enhance the digital resilience of our country in general and of organisations in particular, and insisted as much in the 'Towards a nationwide network of information hubs’[3] CSR recommendation it submitted to the then-Minister of Security and Justice in July 2017. Having correct and reliable information available in time is vital for the digital resilience of public and private sector organisations alike. Sharing and analysing information makes it possible to increase organisations’ resilience against cyberincidents and/or to limit the potential repercussions of such incidents. It is an essential condition if we actually want to exploit the opportunities offered by digitisation to the full, mitigate threats, transact business safely and reliably and protect fundamental rights and values.

Creating a research environment for analysing data breach notifications

The council therefore suggests initiating a project aimed at identifying the value to be gained by making the data breach database available to researchers. The objective of the project will be to identify the insights in connection with privacy and personal data security that may be derived from the notification data, and/or to determine whether (and if so, under what conditions) such analysis might be structurally implemented after the project phase. More information on the structure and framework conditions of the project can be found in **Annex 1** to this letter.

Recommendation

The council has concluded that it would be valuable for the Netherlands to determine the added value of more widespread sharing of data from data breach notifications. The opportunity to learn from incidents in this way has thus far been absent, or nearly so, in the Netherlands. For this reason, the council recommends initiating the research project described above. This project, among other activities, can help us fully capitalise on the opportunities to make the Netherlands an open, secure and prosperous digital nation.

---

[1] Advisory report 'Preparing for digital disruption', the Netherlands Scientific Council for Government Policy (WRR), September 2019

[2] Report ‘Scientific research data breach notification obligation’, Michel van Eeten, Bernold Nieuwesteeg, Michael Faure, November 2018

[3] ‘Towards a nationwide network of information exchanges, advice on information sharing in the field of cybersecurity and cybercrime’, CSR Advisory document 2017, no. 2

Annex 1 contains an explanation on how to create a research environment to facilitate this research. The project will have a term of eighteen months. The Dutch DPA has calculated that it will cost €177,000 to adequately conduct the project and has indicated that it does not itself possess these funds.

We look forward to your response.

On behalf of the Cyber Security Council,

Hans de Jong
CSR co-chair

Pieter-Jaap Aalbersberg
CSR co-chair

CSR Cyber Security Raad

Annex 1: Research environment for the data-breach database

Introduction

The data breach reporting obligation has been in force in the Netherlands since 2016. Organisations are required to report any data breaches directly to the Dutch Data Protection Authority (Dutch DPA), unless the data breach in question is unlikely to result in any risk for the persons whose data were leaked. In addition, in cases where the breach is likely to result in a high risk to the persons involved, the breach must be reported to those individuals as well.

The number of reports is increasing. In 2017, the Dutch DPA received a total of 10,000 reports. By comparison, 11,906 data breaches were reported to the Dutch DPA in the first half of 2019 alone. This works out to around 2,000 reports each month. The total number of data breaches for 2019 will likely amount to some 24,000 incidents, an increase of 14 per cent compared to 2018.

The database comprising the data breach reports contains valuable data. Further analysis of the data is likely to yield insights that will contribute positively to improving cybersecurity. With this in mind, the Dutch DPA wishes to make the database available for the purpose of conducting research. The Dutch DPA is therefore prepared to comply with the CSR's request that it create a research environment in which data breach reports can be analysed. This document sets out the chosen approach. The project will be carried out under the auspices of the Dutch DPA.

The Dutch DPA publishes a data breach report twice a year. These semi-annual reports provide insight into the nature of the reported incidents and offer recommendations aimed at improving security. The report published in September 2019 focused specifically on the healthcare sector. Sharing data breach reports with researchers is expected to facilitate the enrichment of the data breach reports submitted every six months. For the researchers, the project also offers an opportunity to find answers to innovative research questions that will serve to make the Netherlands more secure, by means of analysing the reporting data and enriching the data with other data sets.

Purpose

The Dutch DPA is creating a research environment with the goal of providing scientific institutes with an opportunity to conduct scientific or statistical research and to interpret the data from the data-breach database, for the purpose of arriving at general recommendations and suggestions aimed at improving the security of personal data.

Database held by Statistics Netherlands (CBS)

To establish the research environment, the database containing data breach notifications will be made available to Statistics Netherlands. By sharing this information, the Dutch DPA also makes it possible to link the database to other relevant data sets in Statistics Netherlands' possession for statistical purposes. Statistics Netherlands has a great deal of experience in both the secure storage of data sets of this nature and arranging ‘supervised access’ to those data files.

The Dutch DPA will establish more detailed agreements in this area with Statistics Netherlands. Services provided by Statistics Netherlands in connection with providing external researchers with access to the database will be carried out within what is known as the Remote Access environment.[4]

Personal data in the data set

The Dutch DPA will delete personal data from the data set before submitting the file to Statistics Netherlands. This relates primarily to the name of the contact person at the organisation that is submitting the notification. It may, on occasion, involve other personal data, such as from the person or persons whose data have been leaked. Names of businesses that could potentially be traced to personal information will be deleted as well. The Chamber of Commerce (KvK) number of each business/organisation will be included in the database provided to Statistics Netherlands for the purpose of establishing links to other data sets, such as statistical databases. The data set to be handed over will therefore still contain personal data, for the most part from incidents involving sole traders. Statistics Netherlands will then alter the Chamber of Commerce (KVK) registration number before making the data set available in the Remote Access environment. This will make it more difficult to trace the data back to specific individuals and ensure confidential handling of personal data.

The data breach notifications will be submitted to Statistics Netherlands periodically, with a frequency still to be determined.

Conditions for access to the data set held by Statistics Netherlands (Remote Access environment)

Researchers at scientific institutes may submit a project proposal for research in which they could make use of the data-breach dataset – and possibly other data available from Statistics Netherlands for the purpose of external research. The researchers must be affiliated with institutes in accordance with the conditions established by Statistics Netherlands. If desirable, researchers will be granted conditional access to the database for the purpose of drafting a project proposal. Statistics Netherlands has formulated a number of criteria for conducting so-called microdata research; see https://www.cbs.nl/nl-nl/onze-diensten/maatwerk-en-microdata/microdata-zelf-onderzoek-doen/aanvraag-toegang-microdata.

The following criteria are relevant for the research environment created by the Dutch DPA:

- The institution must have valid authorisation for access to microdata.
- The microdata will be used solely for statistical purposes, meaning they will not be used for administrative, judicial or fiscal purposes or for the purpose of auditing a specific person, company or institution.
- For reasons including the purpose limitation proscribed by the GDPR, the institution must submit a clearly defined project proposal for the research (for proposals involving exploratory studies, the proposal may be more general in nature).
- It must be probable that the Statistics Netherlands microdata will yield answers to at least a significant portion of the research questions.

[4] Statistics Netherlands has a Remote Access environment This environment is intended to provide external researchers with conditional access to the data. Statistics Netherlands also offers Additional Statistical Services. This research will be conducted by Statistics Netherlands and will focus on a specific research question. Through this service, Statistics Netherlands is able to deliver reports to enrich the semi-annual data breach reports from the Dutch DPA.

- In the event that the institution supplies additional files to be linked with Statistics Netherlands microdata, these files must have been lawfully obtained and it must be permissible to share those files with Statistics Netherlands and use them for research purposes.

An agreement will be entered into with the researchers. This agreement will require the researchers to maintain confidentiality with regard to the information in the data-breach database. To that end, the agreement will contain strict provisions concerning confidentiality. It will also state that no business names may appear in the final reports. The Dutch DPA is still in consultation with Statistics Netherlands regarding the precise content of the agreement.

Statistics Netherlands: Additional Statistical Services

In addition to the Remote Access environment, Statistics Netherlands has also defined the Additional Statistical Services (ASD). Within this line of services, Statistics Netherlands conducts commissioned statistical research using the database. These statistics – unlike products resulting from the Remote Access environment – will have a 'Statistics Netherlands quality mark'. Statistics Netherlands is responsible for ensuring the quality of the results. The Dutch DPA will task Statistics Netherlands with conducting additional statistical analyses aimed at the enrichment of the semi-annual data-breach reports.

Within the meaning of the General Data Protection Regulation, Statistics Netherlands acts as controller with regard to these data processing activities.

Costs of the research

Financing must be secured for the costs associated with the statistical work carried out by Statistics Netherlands at the Dutch DPA's behest. The Dutch DPA has not included these costs in its budget.

The costs necessary to prepare the database for research conducted in the Remote Access environment have been set out in the enclosed project budget. The additional costs of research done in Statistics Netherlands' Remote Access environment will be borne by the institutes that submit project proposals. The use of Statistics Netherlands microdata entails certain costs. Based on the project proposal, Statistics Netherlands will provide specification of the costs in connection with each research project. These costs will depend in part on whether Statistics Netherlands will need to conduct research activities for the research in question, and if so, on the specific nature of these activities.

Research committee on data breach notifications

We are establishing a research committee on data breach notifications. This committee will focus on the evaluation of project proposals for research studies to be conducted within the Remote Access environment. The committee will also monitor the progress of the research and evaluate the subsequent results of the studies. In evaluating the proposed research, the committee will ascertain whether the research is in keeping with the objective formulated for it, and whether the research is being carried out within the established framework. These research projects are emphatically not aimed at the publication of the data breach incident reports. Any project proposals having to do with such publication will be rejected. Project proposals with the goal of determining whether publication would be of added value will likewise be considered out of scope. In

the event of a favourable decision by the committee, the researchers will be granted access to the data set within a Remote Access environment for the purpose of conducting their research.

The members of the committee include a representative from the Dutch DPA (chair), a representative from the Council and a representative from Statistics Netherlands. A Dutch DPA employee will bear responsibility for the secretarial duties.

Publication of the results

The results of the research projects will be made public. The Dutch DPA retains the right to publish the results first via the data breach report it publishes twice a year. In cases involving fundamental scientific research, the fact that initial publication may take place via other channels will be taken into account. A solution for this will be sought in close consultation with the committee. Potential solutions will take into account both the Dutch DPA's interest in including results in the data-breach reports and the researchers' interest in achieving academic publication of their research results. Following publication of the results in the data-breach report, the researchers may disseminate the results of the research – with source acknowledgement – via other channels as well. The committee will evaluate whether, based on the nature of the research, publication in the data-breach report is appropriate. Agreements in this area will be made at during the evaluation of the project proposal, i.e. at the start of the project. The reports yielded by the research will contain no company names or unique identifying characteristics of businesses or organisations. Published results will never be traceable to a specific company. Research projects should contribute to improved general insights on information security and lead to recommendations for the improvement of systems. They are not intended as a means to name-and-shame. Likewise, the reports will contain no comments or quotes that may be traced to individuals.

Evaluation

The project will have a term of eighteen months. The project will begin the moment the data are made available via the Remote Access environment for the submission of project proposals. An evaluation will take place once the project has concluded. This evaluation will be prepared by the AP in close consultation with the Council. The objective of the evaluation is to determine whether it will be possible for us to create a structural setting for the research environment.

Costs

The project will be carried out under the auspices of the Dutch DPA. The Dutch DPA has calculated that it will cost €177,000 to adequately conduct the project and has indicated that it does not itself possess these funds. The indicated amount is structured as follows.

Costs to Dutch DPA: preparing the database for transfer (removing identifiable personal data) and carrying out secretarial tasks on behalf of the research committee to be established.	€50,000 (1)
Costs to Statistics Netherlands: Making the database available to the RA environment; intended delivery every six months (12,000). Including processing and linking the general data supplied (3 x 6,000).	€30,000 (2)
Costs to Statistics Netherlands: First trial delivery (4,000), delivery of general report every six months for the enrichment of the data breach reports (3 x 6,000), more in-depth reporting aimed at specific research questions from the Dutch DPA (3 x 25,000).	€97,000
Total funding required	**€177,000**

(1)
These costs do not yet reflect the costs involved in making the general descriptions from the data-breach database suitable for export. An external agency tasked with managing the data-breach database (VISMA) has been asked to draw up a quote in connection with making the additional fields suitable for export. These fields contain further description of the data breach (qualitative descriptions), which may yield valuable data for researchers. While this quote has been requested, the precise costs are not yet known. The Dutch DPA intends to bear these costs.

(2)
Assumes delivery to Statistics Netherlands every six months.