DIF CAPITAL PARTNERS

GDPR – Data Breach Response Policy

2022

Policy Data

Approved by	ExCo
Effective date	19 December 2022
Review cycle	Every other year
Next review date	19 December 2024
Owner	Compliance Team

Document version control

Version number	Publication date	Amendments
V1.0	2018	First version of DIF's Privacy Policies
V2.0	2019	Minor updates DIF's Privacy Policies
V3.0	8 December 2020	Annual review of DIF's Privacy Policies to include minor updates DIF's Privacy Policies, a.o. from annual to bi-annual review
V4.0	19 December 2022	Annual review of DIF's Privacy Policies to include minor amendments.

Contents

1. Scope and purpose of this Policy

1.1 Background of this Policy

As from 25 May 2018, a data breach notification obligation applies throughout the EU. This obligation includes that the DIF Group, as defined in the DIF – GDPR Privacy Policies, will have to notify the Authority in case a Data Breach has occurred that has or may have serious negative consequences for the protection of Personal Data of which DIF is the Controller. In some cases, the DIF Group may also be required to notify all Data Subjects about the Data Breach.

A Data Breach may have serious consequences, not only for Data Subjects, but also for DIF itself, e.g. reputational damage, temporary suspension of the operations, loss of clientele, the imposition of (heavy) fines, etc.

By taking adequate technical and organisational security measures, the DIF Group tries to prevent the occurrence of a Data Breach. We protect our DIF Group Information from loss, theft and unauthorized access and use by maintaining adequate technical security measures in relation to our Systems and by determining rules and procedures about the handling of our Information.

In the event that, despite of the security measures taken by us, a (potential) Data Breach occurs, we must be able to rapidly and adequately respond to such Data Breach. We must therefore obtain all relevant information concerning the Data Breach. Only this way can we comply with the legal obligation to notify a Data Breach to the Authority and (in certain situations) to the Data Subjects. A violation of these obligations can lead to fines and serious reputational damages.

1.2 Purpose of this Policy

The purpose of this Policy is to ensure that we can (timely) comply with DIF's data breach notification obligations. We need to be prepared to adequately respond to any loss, theft, unauthorized access, use or disclosure of Information or our Systems.

This Policy applies to all DIF Employees that have access to and use Information and/or Systems. All Employees should strictly comply with the provisions as set forth in this Policy.

2. Procedure for DIF Employees

2.1 Rules for handling Information

When dealing with Information, Employees shall comply with the following:

- An Employee shall use the Systems.
- In the event that an Employee uses a private computer, USB drive, tablet or other device to use, access, modify or store Information, the employee makes sure to only work in an electronically save environment such as a password protected website (Oracle, PtP, Certify, etc.) and/or CITRIX and/or has Mobile Iron installed.
- In no event shall an Employee send Information to or through his/her private email account/address.
- In no event shall an Employee use services such as DropBox, WeTransfer or WhatsApp for the transfer of Information, unless the Employee has obtained our prior consent thereto.
- An Employee shall maintain log-in details and passwords that give access to confidential Information. It is not permitted to share such log-in details and passwords with other Employees or any other person, not even incidentally.
- An Employee should only bring digital information carriers and/or files outside our premises when strictly necessary and only on carriers provided by us, as this considerably increases the risk of loss and theft of Information.

An Employee should never open emails, of which the sender is or seems unreliable. An Employee should never click on links to websites that are unknown to the Employee and/or seem unreliable. Reference is also made to DIF's IT and Information Security Policy.

2.2 When does an incident constitute a (potential) Data Breach?

A Data Breach may incur when Personal Data is lost, unlawfully destroyed, stolen or is accessed, taken or used by unauthorized persons. A Data Breach may also incur when the Systems are accessed or used by unauthorized persons or in the event that Information and/or Systems have been used for unauthorized purposes.
Examples of Data Breaches are among others:

1. loss or theft of computers, usb-sticks, mobile devices or files (both paper and digital files) containing Information;
2. the discovery that an unauthorised person (this can also be a DIF Employee) has access to Information and/or Systems;

3. the publication of Information on social media;
4. a misdirected email (both internally and externally) containing Information;
5. a security incident at or misuse by our service providers affecting Information;
6. loss or compromise of log-in credentials (username or password) or unauthorised access to log-in credentials, which give access to Information or Systems;
7. (an attempt at) a hack of the Systems.

2.3 Reporting a (potential) Data Breach

Employees play a crucial role in enabling us to adequately and timely respond to a Data Breach. Employees must immediately report an actual, potential or suspected Data Breach in the manner as set out in this Policy. If Employees are uncertain whether the facts of an event, incident, or occurrence constitute a Data Breach, they should nevertheless report such facts.

Employees do not have to determine whether a (potential) Data Breach qualifies as a data breach under the GDPR which has to be notified to the Authority or the Data Subjects. This decision is exclusively reserved for our Compliance Officer.

2.4 When to report?

Every Employee is required to immediately, and ultimately within four (4) hours after becoming aware, report any suspected or actual Data Breach based on the procedure stated below.

2.4 How to report?

Every Employee is required to report any suspected or actual Data Breach to the Compliance Officer who is available every day of the week, 24 hours a day (24/7) by email to f.kuiper@dif.eu or k.fluks@dif.eu or by phone at +31 639007496 or k.fluks@dif.eu or by phone at +31 642111189.

Every Employee that notifies a Data Breach to the Data Protection Officer must hand over a completed copy of the DIF – GDPR – Data Breach Response Form, as attached hereto as **Annex 2**. The Employee shall do so promptly after having reported the Data Breach. The Employee shall complete the DIF – GDPR – Data Breach Response Form as much as possible. If certain facts are not yet clear at the moment that the Employee completes the DIF – GDPR – Data Breach Response Form, the Employee shall inform the Compliance Officer of these facts as soon as these have come under the attention of the Employee.

The Employee shall fully cooperate with the Compliance Officer and shall provide all the information requested by the Compliance Officer.

3. Task of the Compliance Officer

As soon as the Compliance Officer has received a DIF – GDPR – Data Breach Response Form, he will review the questionnaire to see if all questions have been answered sufficiently. In case relevant information is missing, the Compliance Officer will obtain the missing information from the Employee.

Once the DIF – GDPR – Data Breach Response Form has been fully completed, the Compliance Officer will assess whether:

1. the Data Breach qualifies as a data breach under the GDPR, and if so, whether:
2. the Data Breach should be notified to the Authority; and
3. whether the Data Subjects should be notified of the Data Breach.

In all cases, the Compliance Officer shall record information about the Data Breach in the internal Data Breach Register.

The Compliance Officer shall make this assessment, taking into account any Policy Rules of the Authority and this Policy, within twenty-four (24) hours after receipt of the Data Breach Questionnaire.

3.1 Does the Data Breach qualify as a Data Breach under the GDPR?

This question should be answered by the Compliance Officer in three parts:

1. *Was there a breach of the security measures?*

The first question that needs to be answered is whether our technical and/or organisational measures were breached. There must be an actual breach of the security measures. A treat of a breach is insufficient. The precautionary measures taken to prevent a breach of the security measures must have failed. Examples of a breach of security measures are: (i) a lost USB-stick; (ii) a stolen computer; (iii) a hack; (iv) a malware infection or (v) a fire in a data center.

2. *Was Personal Data exposed to loss or destruction?*

Secondly, it must be assessed whether the breach on our technical and organisational security measures resulted in the loss or destruction of Personal Data. A Data Breach only qualifies as a data breach for the purposes of the GDPR in the event that the breach of the security measures resulted in the actual loss or destruction of Personal Data. For example, if Personal Data was destroyed, but could be recovered using a back-up, the incident does not qualify as a data breach under the GDPR.

3. *Can it be ruled out that Personal Data were processed unlawfully?*

The third relevant question is whether it can reasonably be ruled out that Personal Data were Processed unlawfully. If it cannot reasonably be ruled out that the breach of the security measures resulted in the unlawful Processing of Personal Data, the Data Breach is a data breach for the purposes of the GDPR. Examples of unlawful Processing include the unauthorized access to or destruction of Personal Data. If, also as example, an Employee gave out his/her user name and password to a third party, but it can be established by using server logs that no one used these credentials to log in, the incident does not qualify as a data breach under the GDPR.

In case of doubt, the Compliance Officer should qualify a Data Breach as a data breach under the GDPR.

3.2 Notification of the Authority

In the event that the Compliance Officer has determined that the Data Breach qualifies as a data breach for the purposes of the GDPR, he shall subsequently assess whether the Data Breach must be notified to the Authority.

The Compliance Officer shall report the Data Breach to the Authority. If the Personal Data affected by the Data Breach are of a sensitive nature, we consider that it is likely that the Data Breach will result in a risk to the rights and freedoms of the Data Subject. Accordingly, the Data Breach will have to be reported to the Authority.

The Compliance Officer shall in each specific case assess whether the Personal Data are of a sensitive nature, which may include:

- special categories of Personal Data (personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data, data regarding health, sex life or sexual orientation and data relating to criminal convictions and offences);
- data regarding the financial or economic situation of the Data Subject(s);
- data which may lead to stigmatisation or exclusion of the Data Subject(s);
- user names, password and other log-in information;
- data which may be used for identity fraud, such as social security numbers or copies of passports.

If the Personal Data affected by the Data Breach do not fall in one of these categories, the Data Breach may still result in a risk to the rights and freedoms of the Data Subjects (and need to be reported to the Authority) based on the nature and size of the Personal Data. The following considerations should be taken into account:

- If the volume of the compromised Personal Data and/or the Data Subjects increases, it will become more prone to abuse and will more likely cause harm for the Data Subjects.
- If the compromised Personal Data are used for taking decisions about Data Subject, this increases the impact. For example, if a hacker has access to and potentially is able to change data in a database used for assessing credit worthiness, that will have more impact than if that same database would be used for marketing purposes.
- If the compromised Personal Data is used throughout a chain of service providers, it becomes harder to manage the consequences of that data being lost or altered, which increases the impact of the Data Breach.
- Certain Data Breaches involve a higher risk of abuse (e.g. a hack).

3.3 How and when to notify the Authority

If the Compliance Officer concludes that a Data Breach must be notified to the Authority, such notification must be done as soon as possible but in any case within 72 hours after the first discovery of the Data Breach. This report shall be submitted in line with the “Beleidsregels voor toepassing van artikel 34a van de Wpd” as issued by the Dutch Data Protection Authority. If the Compliance Officer does not have all the relevant information regarding the Data Breach available within this timeframe, he shall nevertheless notify the Authority of the Data Breach and supplement this notification as soon as he has received all relevant information. If the Data Breach is not reported to the Authority within the 72-hour period, the report shall specify the reasons for the delay.

The notification to the Authority must at least contain information on:

- the nature of the Data Breach and the categories and approximate number of Data Subjects concerned;
- the categories and approximate number of Personal Data records concerned;
- the name and contact details of the Data Protection Officer (or other contact person) where further information on the Data Breach can be obtained;
- the recommended and taken measures in order to address the Data Breach and to mitigate the possible adverse effects of the Data Breach; and
- the actual and likely consequences of the Data Breach.

If new relevant facts or details about the Data Breach are discovered or revealed after the Data Breach was notified to the Authority, the Compliance Officer will amend or supplement the Notification Form as soon as he obtains such relevant facts or details.

3.4 Notification(s) to Data Subjects

If the Compliance Officer has determined that a Data Breach qualifies as a Data Breach under the GDPR, it should also be determined whether the Data Breach should be notified to the Data Subject(s).

Under the GDPR, a Data Breach needs to be notified to the Data Subject(s) when the breach is likely to result in a high risk to the rights and freedoms of the Data Subjects.

The Data Subjects do not have be notified when:

- The Personal Data affected by the Data Breach were protected by appropriate technical and organisational measures that render the affected Personal Data unintelligible (e.g. encryption, remote wiping, hashing/pseudonymisation) for any unauthorized person.
- When we have taken measures following the identification of the Data Breach, which ensure that the high risk to the rights and freedoms of the Data Subjects is no longer likely to materialise (for example if the Personal Data were remotely wiped before unauthorized access took place, which can be demonstrated by means of logging).
- This would involve disproportionate effort. In this case, the Compliance Officer shall publish a public communication regarding the occurrence of the Data Breach (on our website). The Compliance Officer shall not easily conclude that notifying the Data Subjects involves a disproportionate effort.

If and when the Compliance Officer determines that a Data Breach shall be notified to the Data Subjects:

- the Data Subject(s) should be notified without undue delay;
- the notification to the Data Subjects shall be in clear and plain language;
- the notification to the Data Subjects shall be done personally, by email and/or by telephone. Only if the Compliance Officer establishes that a personal notification is not possible, or would constitute a disproportionate effort (see above), a public notification (e.g. a letter to all customers or a publication on the website or in a newsletter) will suffice; and
- the Data Subject(s) shall be informed on at least the following aspects:
  - the actual and likely consequences of the Data Breach as well as the way in which we have has dealt with or intend to deal with these consequences.
  - the name and contact details of Compliance Officer where further information on the Data Breach can be obtained; and
  - the recommended measures and measures taken by us in order to mitigate the possible adverse effects of the Data Breach.

3.5 Data Breach Register

The Compliance Officer shall maintain an internal Data Breach Register in which it records all Data Breaches (also the Data Breaches that have not been notified to the Authority and/or the Data Subjects).

This Data Breach Register shall include at least:

- facts and information about the nature and circumstances of the Data Breach;
- the effects of the Data Breach;
- the measures taken to mitigate and remedy the possible adverse effects.

The Compliance Officer will store the information of the Data Breach Register for at least 10 years, provided that the Data Breach Register contains personal Data. In the event that the Data Breach Register does not contain personal data, there will be no storage limitation period.

The Compliance Officer will review this internal Data Breach Register periodically to determine whether there are reasons to investigate amending our technical and/or organisational security measures.

4. Violations

A violation of this Policy shall be subject to disciplinary measures and/or applicable sanctions including the termination of employment, to the extent permitted by applicable (employment) laws and regulations. In addition, we reserve the right to pursue any and all remedies allowed by applicable laws or regulations.

Annex 1

Definitions

In this Policy, the following terms shall have the following meanings:

Authority	the Dutch Data Protection Authority (https://autoriteitpersoonsgegevens.nl/en)
Compliance Officer	Frits Kuiper (E f.kuiper@dif.eu, M +31 639007496)
Controller	means a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
Data Breach(es)	means every breach of security measures (including technical and organisational) leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
Data Breach Register	means the internal register listing all Data Breaches.
Data Subject(s)	means the individual(s) whose Personal Data is concerned.
Employee	means every person employed by the DIF Group and every person, who is not employed by the DIF Group but performs work activities for the DIF Group on the basis of a contract, such as: • temporary workers; • consultants; • directors; • self-employed persons; • seconded personnel and personnel hired in; and • interns.
GDPR	means the General Data Protection Regulation (Regulation (EU) 2016/679).
the DIF Group Information	means (non-public) information about or related to the DIF Group, its customers and/or Employees, which information may include Personal Data.
Policy	this Data Breach Response Policy.
Personal Data	every data or information that relates to an identified or identifiable natural person, such as Employees or Investors or Commercial Counterparties of the DIF Group, including but not limited to: a name, address, place of residence, telephone number, social security number, bank account number, gender, health data, financial data and insurance information, photo and IP-address.
Policy Rules	the most recent version of the policy rules regarding the data breach notification obligation, issued by the Authority, as applicable.
Processing	every act in relation to Personal Data, including but not limited to: collecting, using, storing, modifying, deleting, making available, transferring, spreading, deleting, and combining.
Processor	means a natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller
Systems	means any computer, computer network, computer application, storage device or media, mobile computing device or any other information technology hardware or software, owned, licensed or leased by the DIF Group, or operated by a third party on behalf of the DIF Group, that processes, stores or transmits the DIF Group Information and is approved by the DIF Group.

Annex 2

DIF – GDPR – Data Breach Response Form

A Data Breach may incur when Information is lost, unlawfully destroyed, stolen or is accessed, taken or used by unauthorized persons. A Data Breach may also incur when the Systems are accessed or used by unauthorized persons or in the event that Information and/or Systems have been used for unauthorized purposes. Examples of Data Breaches are among others:

1. loss or theft of computers, usb-sticks, mobile devices or files (both paper and digital files) containing Information;
2. the discovery that an unauthorised person (this can also be a DIF Employee) has access to Information and/or Systems;
3. the publication of Information on social media;
4. a misdirected email (both internally and externally) containing Information;
5. a security incident at or misuse by our service providers affecting Information;
6. loss or compromise of log-in credentials (username or password) or unauthorised access to log-in credentials, which give access to Information or Systems;
7. (an attempt at) a hack of the Systems.

Instruction in case of a (potential) Data Breach;

1. The DIF employee must report the Data Breach personally, by e-mail or phone, to the relevant Compliance Officer (Frits Kuiper, M: +31 (0)6 39007496 or f.kuiper@dif.eu).
2. Fill in this DIF – GDPR – Data Breach Response Form.
3. Mail this Form to the Compliance Officer.

Please be aware that every DIF Employee is required to immediately, and ultimately within four (4) hours after becoming aware, report any suspected or actual Data Breach.

For definitions of the terms used in this Form, please be referred to the **DIF – GDPR – Data Breach Response Policy**.

Thanks for your cooperation and alertness,

The Compliance Team

	QUESTIONS	ANSWERS EMPLOYEE
1.	Name and function of the reporting DIF employee.	
2.	Does this concern a loss or theft of a USB-stick, computer, tablet, telephone or other device? If yes, please describe how and where the loss or theft took place and *please continue to question 10.*	
3.	Was there another Organisation involved, e.g. as a Processor? If so, please provide (1) the name of the organisation involved and (2) the service they provide.	
4.	What is the (assumed) date and time of the start and the discovery of the Data Breach? Please try to be as specific as possible.	
5.	Describe the nature of the Data Breach, e.g. accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.	
6.	Please summarise the relevant facts of the Data Breach, e.g. what happened, when and how did you become aware of the Data Breach?	
7.	What type of Data Subjects were or may be affected by the Data Breach, meaning who's Personal Data was breached, e.g. DIF's Employees or DIF's Counterparties?	
8.	How many Data Subjects were or may be affected by the Data Breach?	
9.	Please describe the sort of Personal Data which is affected by the Data Breach, e.g. birth of date, social security number, tax identification number or financial data etc.	

10.	Was the Information affected by the Data Breach protected by security measures? (for example, was the Information encrypted, was the device protected with a password)	
11.	What immediate measures were taken when the Data Breach was discovered?	
12.	Please describe in your own words what the consequences of the Data Breach could be?	
13.	Date of this Form:	