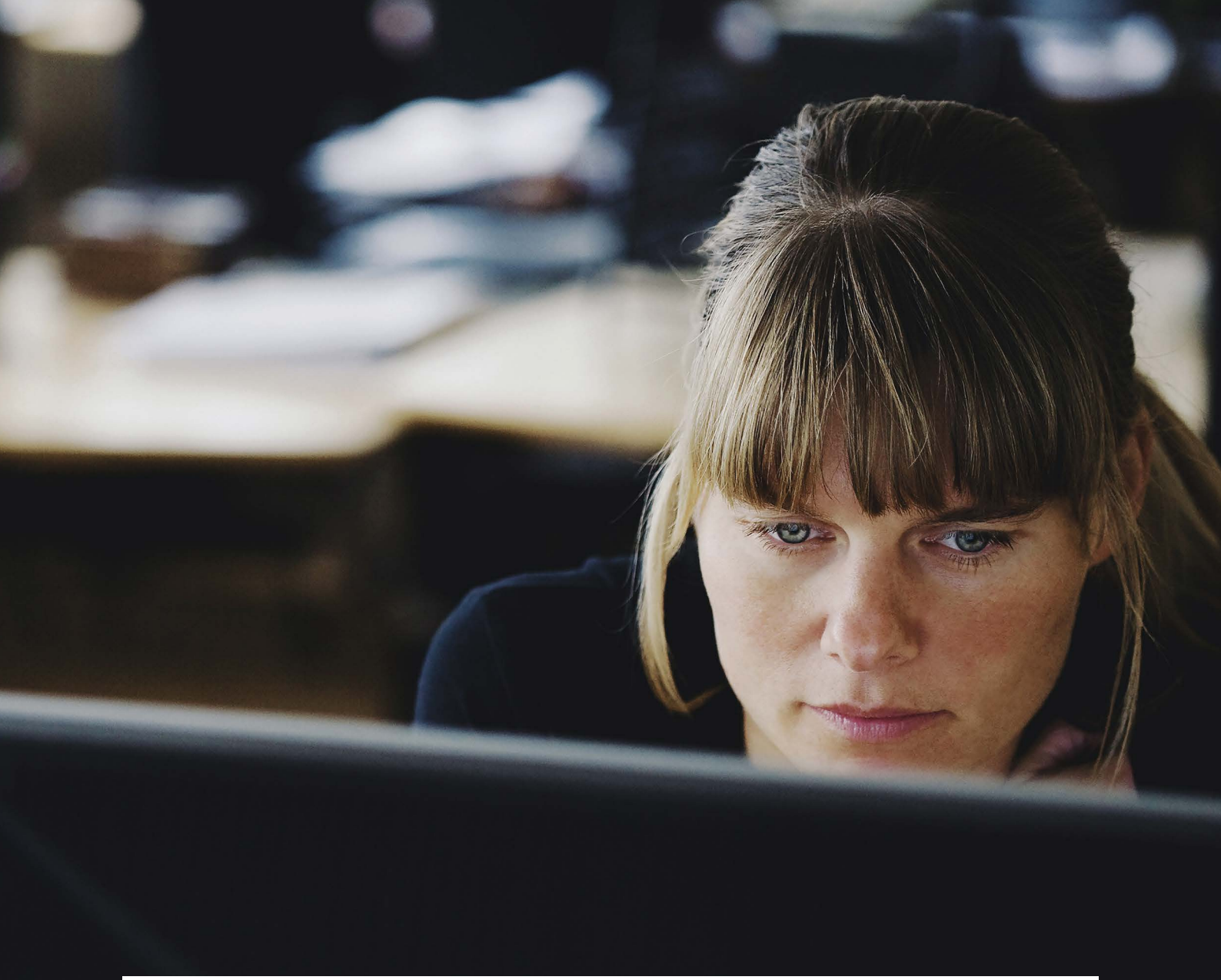


GUIDE

Reporting of Security Flaws

KMD

Guide to Reporting of Security Flaws

One of the fundamental prerequisites for the success of the digitalization process is that customers and citizens trust the digital solutions that support the digital Denmark. In other words, good IT security is a decisive factor.

The companies and authorities will therefore very much like to hear from you if you become aware of any errors or security flaws in systems that may lead to a security or data breach.

All companies and authorities which have adopted the Danish ICT Industry Association Code for Reporting of Security Flaws will strive to manage your notification in accordance with the following guide.

We recommend that you study the guide carefully to comply with the parts that concern you as an informer.

WHEN TO REPORT?

- You are requested to report immediately when you detect a security flaw which, in your opinion, may lead to the abuse of information that appears by nature to be confidential. An example of this can be if you see information about other citizens that, in your opinion, you should not be able to see/access.
- At an overall level, we would like to hear about inadvertent access to personal data or sensitive company information. Such examples include:
  - If you have received or been granted access to other citizens' personal data
  - If it is possible to change the rights or otherwise access other users' user accounts/details
  - If you have become aware of vulnerabilities or possible exploits that can be used to access data that are otherwise inaccessible.

WHAT DO WE NEED TO KNOW?

- In the greatest possible detail, please provide a description of the problem/error you have detected.
- Your notification should preferably contain the following information:
  - How you became aware of the problem/error
  - What, in your opinion, is the nature of the error/security flaw
  - Where you detected the problem/error/security flaw
  - Screenshots of the problem/error/security flaw.
- Your contact details.
  - We accept and respect if you request anonymity within the framework of the law, but we urge you to send us your contact details. You may report security flaws in your name or anonymously through the KMD Whistleblower Arrangement. Please find more details on the arrangement **here**

WHAT SHOULDN'T YOU DO?

- You should not take advantage of any error/security flaw you may have observed for the purpose of accessing data.
  - It is naturally possible for you to be granted access to data that does not concern you through no fault of your own. What is vital is that you do not explore the security flaw and take advantage of it to access any additional data.
- Once we receive your notification, we will immediately, depending on the scope and severity of the security flaw, initiate the rectification work. We appeal to you that you do not contribute yourself to exacerbating the consequences of the identified security flaw – for example, by going to the media with your knowledge of the security flaw, while we are processing your notification. This also applies to social media.
  - Others may take advantage of the security flaw. Therefore, it is of decisive importance that we get an opportunity to solve the problem before it becomes public knowledge. This makes it possible for us to limit the damage – also for anyone who has possibly been affected.
- If you choose to contribute to spreading information that has inadvertently become accessible as a result of the identified security breach, we may be forced to consider you complicit in hacking and possibly proceed by reporting you to the police.

WHERE SHOULD I REPORT?

- Please send the notification through the KMD Whistleblower Arrangement **here**
  - We kindly ask you to inform us of the problem as quickly as possible and without undue delay. It is vital that we get an opportunity to solve the problem as quickly as possible.

IS THERE A REWARD?

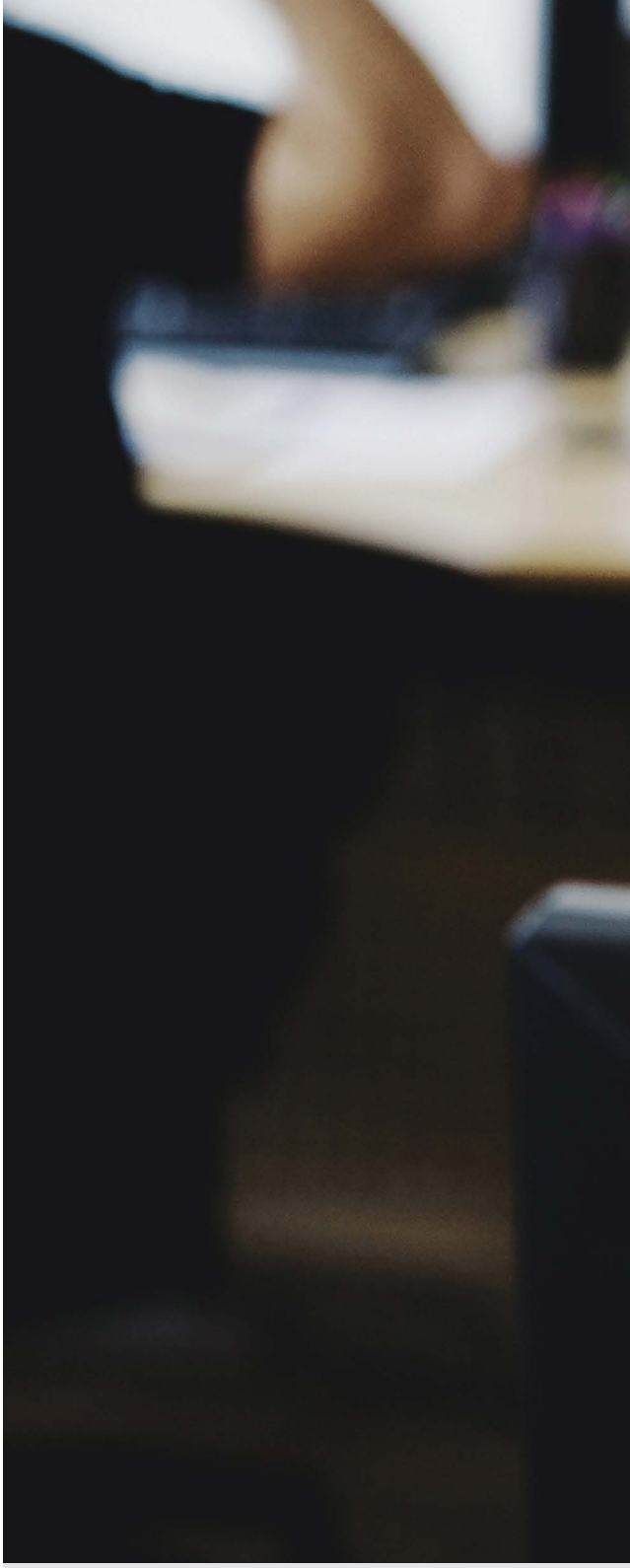
- KMD does not have a reward system for persons reporting a security flaw but may subject to exceptional circumstances choose to give a reward.

WHAT DO WE NOT NEED TO KNOW ABOUT?

- Ordinary program errors that do not lead to inadvertent access to personal data, as described above.
- Ordinary technical inquiries, e.g., concerning program errors, should be directed to our general support by completing the **contact form** on our webpage or by calling +45 4460 0000.

WHAT HAPPENS AFTER YOU SEND US YOUR NOTIFICATION?

- We will take your notification seriously and process it as soon as we receive it.
- When using the KMD Whistleblower Arrangement, you will always, within 48 hours of sending your notification, receive a confirmation that we have received it.
- Also, you will get feedback within two weeks, which will describe what we have done with your notification. The feedback will also indicate if you should expect to hear something more from us, or if the case is closed.
- There may be a duty to report the security flaw/data breach to the Danish Data Protection Authority or other public authorities. As a rule, this duty rests on the data controller and data processor, not on you as a citizen/informer. Once you have notified us of the data breach, we will proceed with the notification, if any, to the Danish Data Protection Authority.



Lautrupparken 40-42
2750 Ballerup
Tlf. 4460 1000
www.kmd.dk