kubrick

Handling Nexo Bank's data breach: Obtaining Consent

14 April 2024

Insert slide title here

A guideline on how Nexo Bank can obtain consent for data processing

- Transparency and Clarity
- Freely given consent
- Specific consent
- Explicit consent
- Free and unambiguous consent
- Records of consent
- Easy withdrawal of consent

Response to Data Subject Access Requests:

-There should be a clear process and regulations already set up for how to response to a breach- These should be set up and enforced by the Data Compliance Manager.

The Data Protection Officer (DPO) is generally responsible for establishing, reviewing, and advising on the overall processes for responding to DSARs to ensure they comply with GDPR. This includes setting out how requests are recognized, how personal data is to be gathered, and the manner in which responses are to be formulated and provided.

The actual handling of DSARs, including receiving requests, verifying the identity of the requester, gathering the necessary information, and communicating with the data subject, may be performed by Data Compliance Managers or other designated staff within the organization. These tasks are operational and require a good understanding of the organization's data processing activities.

GDPR requires that responses to DSARs be provided without undue delay and in any event within one month of receipt of the request. Depending on the number and complexity of the requests. Here 100 000 breaches were made so if all affected customers were to request for their data this would be quite time consuming.

Information should be provided in a concise, transparent, intelligible, and easily accessible form, using clear and plain language. You want to enforce transparency with the data.

Ensuring Valid and Lawful Consent:

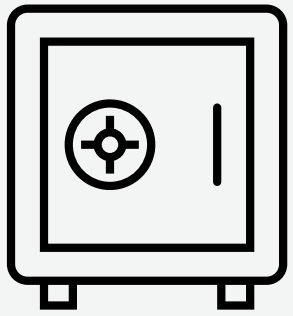
Consent Reviews:

- These should be regular or at least when there is a big change to data processing or regulatory requirements
- It should be detailed and should assess how clear consent requests are, methods used and the purpose
- Should be documented including reasons for change
- A compliance check

Ensuring Valid and Lawful Consent:

Clear Opt-Out Mechanisms:

- Accessible
- Simple and straightforward
- Fast responses
- Data removal
- segmentation



Ensuring Valid and Lawful Consent:

Data Protection Impact Assessments (DPIAs):

- Early assessment
- Identify risks
- Periodic reviews

How should the bank respond to the DSARs

- Loyalty and trust, ensure transparent communication
- Report to data controller and Regulator (ICO)
- Review data security processes and encryption
- Have a privacy programme plan
- Training within company, opportunity for improvement