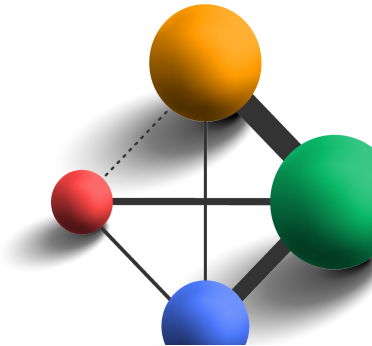
SalesColors

	Process steps	Activity	Responsible person
1	A (possible) data breach is discovered	• Immediately report a (possible) data breach internally • Inform the responsible Contact Person; the responsible Contact Person is the designated Data Protection Officer, failing which this task will be performed by the CEO of Sales Colors.	• Employee hat first identifies the (possible)data breach.
2	Assess the data breach	• Investigate the security incident • Investigate whether personal data has been lost or can be used unlawfully • Assess who or which departments within the organization are involved. • Assess whether an external processor or other third party is involved in the incident. If so, they should be informed and involved in the process.	• Data Protection Officer[i]
3	End the data breach	• Stop the data breach where and when possible. • Take other measures to limit the data breach and the resulting damage. • Record in the file the actions of the analysis and measures taken.	• Data Protection Officer.
4	Determining the impact of the data breach	• Investigate the data breach and its consequences. • Investigate the nature of the data that has been leaked. E.g. Health Data, passwords, data about financial situation or that can lead to stigmatisation/abuse. • Investigate the extent of the leaked data. • Assess what impact the leakage could have on the people involved. • Determine what the adverse consequences may be.	• Data Protection Officer.
5	Establish, Report and Recover Approach	• Determine approach and the necessity of informing DATA PROTECTION AUTHORITY (DPA, in Dutch: "Autoriteit Persoonsgegevens"). • Determine the approach/inform those involved. • Determine actions for aftercare stakeholders. • Determine actions for the interest of the organization. • Define security improvement actions.	• Data Protection Officer in consultation with the CEO of Sales Colors.
6	Report DPA / AP[ii]	• If it is decided to inform DPA / AP, this must be done within 72 hours after discovery of the data breach. • Notification via the website of the DPA / AP; the Data Leak Report Form can be used if necessary.	• Data Protection Officer in consultation with the CEO of Sales Colors.
7	Report those involved[iii]	• Notification via, for example, letter. • Communicate what has happened, which personal data have been affected and what the possible consequences of the data breach may be. • Informing about the measures that the organization is taking, and that the person	• Data Protection Officer in consultation with the Marketing Communications Department and the CEO of Sales Colors.



		concerned can take, to prevent damage.	
8	Repair and recovery.	• Fix the data breach. • Improve security. • Provide aftercare to those involved.	• Data Protection Officer
9	Optimize the security and data breach process.	• Record, evaluate and improve data breach security and notification process.	• Data Protection Officer in consultation with the CEO of Sales Colors.

[i] *If no Data Protection Officer is appointed, the CEO of Sales Colors will function as such and shall fulfill the relevant duties.*

[ii] *Notification to the Dutch Data Protection Authority can only be avoided if it is unlikely that the data breach will cause a high risk of violation of the rights and freedoms of the data subjects. This partly depends on the nature and scope of the leaked personal data. If, for example, only the address details of a small group of data subjects have been leaked, it is unlikely that there is a high risk.*

[iii] *If the data breach is likely to cause a major risk to the rights and freedoms of the data subjects, the data breach must also be reported to the data subjects. If, for example, health data has been leaked, the leak will in any case have to be reported to them. The CEO of Sales Colors will always have to be involved in the consideration as to whether the leak causes a high risk.*