



TLP:CLEAR = Publicly



Security Breach (incl. privacy breach)

DSOP Control Information Common Standard - Operational processes



Purpose of routine



- To ensure that the party which discovers the security breach (privacy breach, cyber-attack, etc.) takes immediate measures on their side to prevent the breach from inflicting more harm. For this purpose, the party shall follow their internal routines.
- If the party sees it probable that other parties in the solution must also take immediate measures on their sides to prevent further harm linked to the security breach, the routine shall facilitate continuous updated and available contact information. This contact list, which shall only be used in the event of a security breach, will contain the name of the party, the name of the contact person, a phone number, and an e-mail.
- To establish an emergency action group* with involved parties responsible for continual handling of the security breach and writing an incident report.

* The group shall be established within working hours, as soon as Bits have been aware of the breach. Bits shall ensure that the emergency action group is established and will summon the first meeting - where it will be decided which party in the group will be Bits' contact person. Bits will attend the introduction in the first meeting but will not be an active participant in the group. It is the group itself that shall be responsible for the handling and follow-up of the security breach. The group shall remain active until the incident report is handed to the affected parties.

Security Breach

Process overview



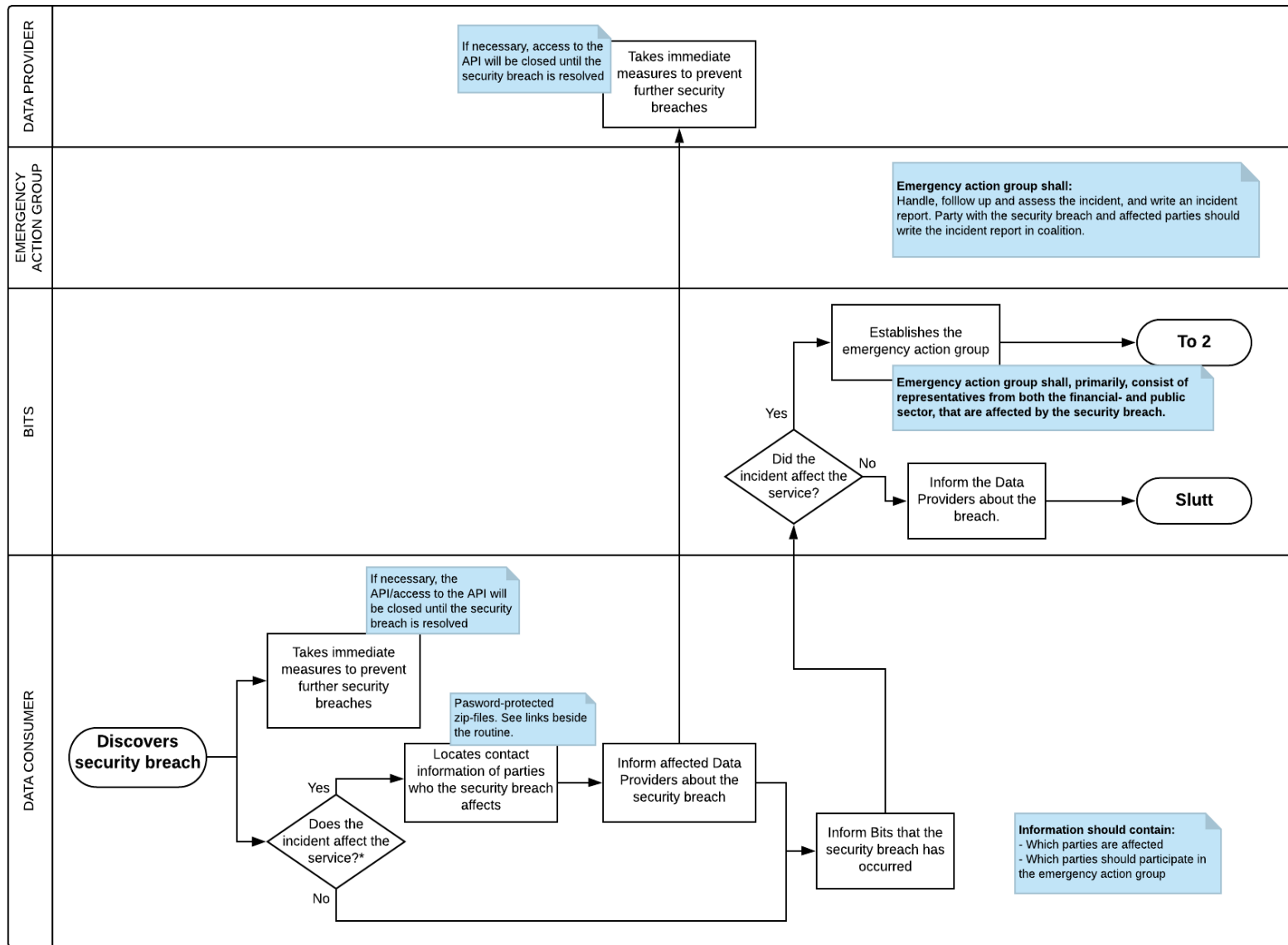
1.a
Security breach is discovered by a data consumer

1.b
Security breach is discovered by a data provider

2
Emergency action group investigates the incident

1.a

Security breach discovered by data consumer



For security breach:

[Link to contact information \(password is specified in the SLA for Control\)](#)

For privacy breach:

[Link to contact information \(password is specified in the SLA for Control\)](#)

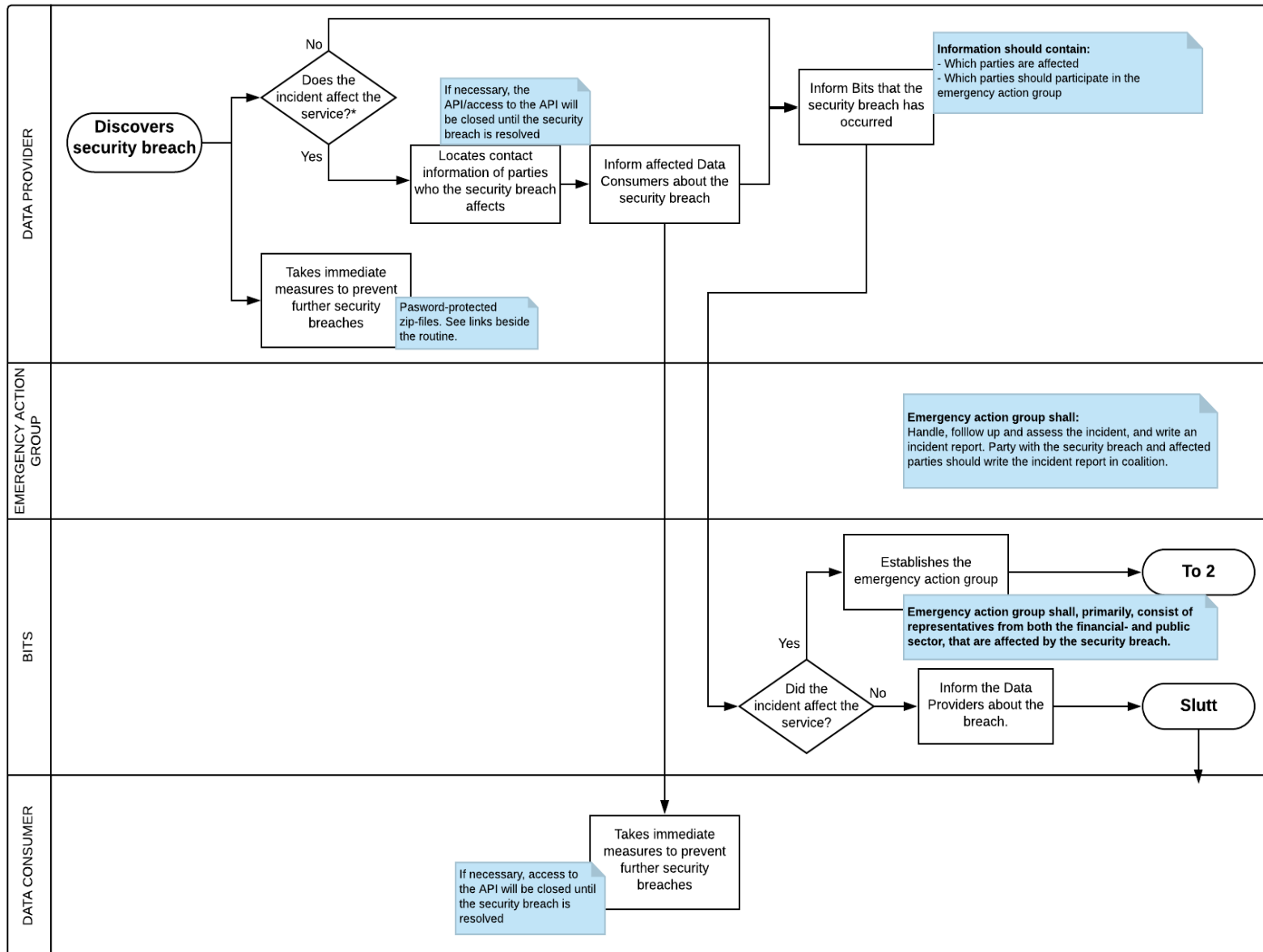
If the security breach also applies to privacy breach, both contact lists must be used.

Otherwise, if the breach only applies to one of them, use the contact list that applies to the breach.

*If there are any doubts, the Data Consumer should inform the Data Providers.

1.b

Security breach discovered by data provider



For security breach:

[Link to contact information \(password is specified in the SLA for Control\)](#)

For privacy breach:

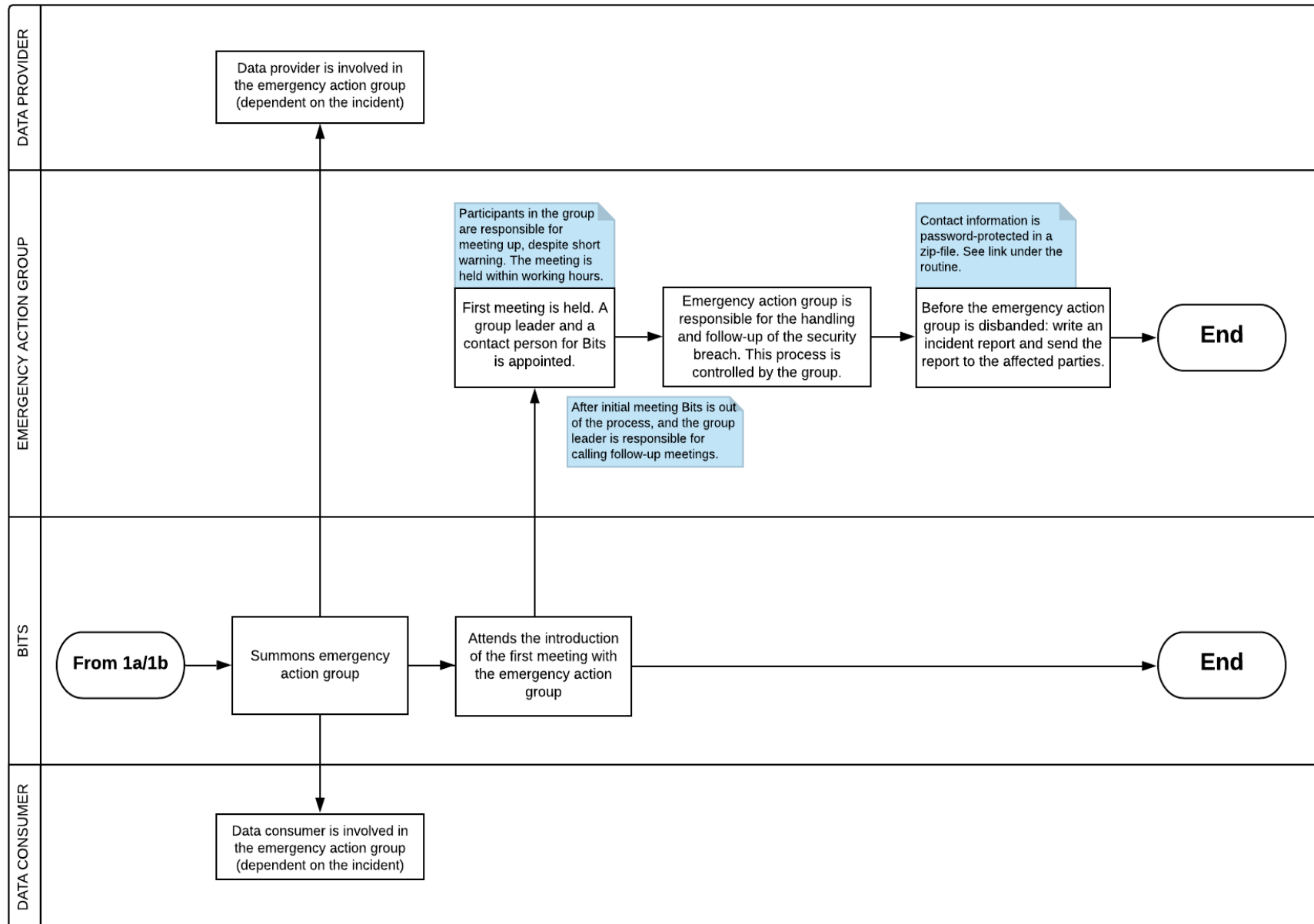
[Link to contact information \(password is specified in the SLA for Control\)](#)

If the security breach also applies to privacy breach, both contact lists must be used.

Otherwise, if the breach only applies to one of them, use the contact list that applies to the breach.

*If there are any doubts, the Data Providers should inform the Data Consumers.

Emergency action group investigates the incident



The image features a central logo for 'DSOP' in a bold, blue, sans-serif font. The letters are outlined and set against a background of a stylized globe with glowing white lines and dots. The globe is positioned on the right side of the frame. The background is a light blue gradient with faint binary code (0s and 1s) and a grid pattern. The entire scene is framed by a dark teal border.

DSOP

DIGITAL SAMHANDLING OFFENTLIG PRIVAT