Contingency plan

This Contingency Plan provides guidance for our team in the case of trouble delivering our business functions because of disruption, compromise, or failure of any component of the GDPR-Portal. As a general guideline, we consider "disruption" to be more than 30 minutes of unexpected downtime or significantly reduced service for customer applications.

Scenarios where that could happen include unexpected downtime of key external services, data loss, or high-severity security incidents.

Recovery objective

Short-term disruptions lasting less than 30 minutes are outside the scope of this plan. (See SLA instead.)

More than 4 hours of the GDPR-Portal being offline is unacceptable. Our objective is to recover from any significant problem (disruption, compromise, or failure) within that span of time.

Contingency plan outline

The following describes how we approach solving any given disruption.

Activation

When any GapSolutions team member identifies a potential contingency-plan-level problem, they should begin following this plan.

The priority is to notify the following people. They are each authorized to decide that GapSolutions needs to activate the contingency plan. To contact them, use any normal means of communication (e.g. phone, e-mail, chat).

- Per Løkken | (+45) 7192 9350 | pl@GapSolutions.dk
- Jacob Barlach | (+45) 2523 2316 | jb@GapSolutions.dk

Are neither Per nor Jacob available, any GapSolutions employee can initiate the Contingency Plan.

If either of these cases the contingency plan will be activated, and the following steps will be processed:

Notification

Employees and partners of GapSolutions are notified of the issues within 15 minutes of identifying the disruption.

All customers or users that submits questions or concerns should be notified of the activation of the Contingency plan as well.

Recovery

First a backup procedure is initiated. The IT team assesses the situation and works to recover the system from the most recent stable backup (See backup strategy) and the following the prioritized solution scenarios (See prioritized solutions). See the list of external dependencies for procedures on how to recover from problems with external services.

The backup strategy consists of the following:

Backup Strategy:

Time:	**What we do:**
0 – 7 days	Point in time recovery
7 – 14 days	Nightly backup
14 days – 3 months	Weekly backup
3 – 6 months	Monthly backup
0 – 2 years	Yearly backup

Prioritized solutions:

Level/Scenario:	**What we do:**	**Time:**
1	Redeploy to same region	60 min.
2	Redeploy to another region	60 – 120 min.
3	Redeploy to another Iaas* provider	Max 24 hours

* Infrastructure as a Service

If level 1 does not work, move on to level 2, if level 2 does not work, move on to level 3.

Continuous communications

At least once an hour: Post a brief update to 'Status Page' on the public web site. To keep customers informed, that we are aware and working on solving the problem.

If the Main website/domain "GapSolutions.as" is down or unavailable, alternative domains will be used. Either 'GapSolutions.dk' or 'GAPSOLUTIONS.as'.

Reconstitution

The IT team will redeploy new versions of both web server and database servers, from the latest stable backups. The IT team will also test and verify that everything is working.

If the IT team declares that recovery efforts are complete, they will notify all relevant people, which typically includes:

- Customers
- Partners

- Employees

External dependencies

The GDPR-Portal depends on several external services. In the event one or more of these services has a long-term disruption, the IT team will mitigate the impact by following the steps below:

Bitbucket

If Bitbucket becomes unavailable, the live GDPR-Portal will continue to operate in its current state. The disruption would only impact the team's ability to update the GDPR-Portal.

Disruption lasting less than 7 days

The IT team will postpone any non-critical updates to the platform until the disruption is resolved. If a critical update must be deployed, the IT team will:

1. Locate a copy of the current version of the required git repository by comparing last commit times of all checked out versions on GapSolutionss local systems.
2. Perform the change on the local copy of the repository (if the update requires a change to git-managed source code), or use local copies of the repository instead of remote Bitbucket repository references (if the update depends on remote repositories but implies no change to those repositories).
3. Manually deploy the change to the server.

When the disruption is resolved, the IT team will push any changes to the appropriate repositories in Bitbucket to restore them to the current stable state.

Disruption lasting more than 7 days

The IT team will:

1. Deploy and configure GitHub
2. Migrate repositories from local backups to GitHub

After these steps are complete, updates will be deployed per usual policy using GitHub in place of BitBucket.

Hetzner

In case of a significant disruption the IT team will deploy a new instance of the entire system to a different region.

If all regions are disrupted, IT team will deploy the system to another IaaS provider (such as Microsoft Azure, Digital Ocean or AWS).

Flowmailer

If Flowmailer becomes unavailable or unable to deliver mail and the current load is under 10.000 mails, then the mail service will be transferred to a Microsoft SMTP server. In case the current mail load is above 10.000 mails per day, then GapSolutions will set up an internal SMTP server at Hetzner and use this instead.

Test

Every 6 months the contingency plan is tested, to make sure that GapSolutions is ready if one day the contingency plan is needed.

All 3 scenarios as seen under the 'Recovery' section will be tested. Redeployment in the same region, another region and to another IaaS[1].

[1] Infrastructure as a Service