European Supervisory Authorities have shed light on their initial enforcement priorities. The French CNIL publicly acknowledged the difficulty of complete GDPR compliance, stating that companies not yet fully compliant “can expect to be treated leniently initially provided that they have acted in good faith.” The Dutch AP has similarly stated that “fines will only be imposed at the beginning if it is obvious something is very wrong” in response to the fears of local municipalities.

What do “acting in good faith” and “very wrong” mean? Follow our handy flow chart to see if you’re likely to come into the crosshairs of European regulators:

- **APPOINTED DPO:** Have you appointed a data protection officer (DPO) who is responsible for processing activities?
- **DATA INVENTORY AND MAPPING:** Do you know what data you collect and hold, where it is stored, how it is used, and how it is secured?
- **GAP ANALYSIS:** Have you completed a fundamental assessment, comparing internal practices to the requirements of the GDPR?
- **PRIVACY NOTICE (TRANSPARENCY):** Does your privacy notice clearly explain your privacy practices and explain the rights of your data subjects?
- **LAWFUL BASIS FOR PROCESSING:** Have you identified a lawful basis for processing personal data?
- **SECURITY:** Do you have and maintain a clear security policy, including industry standard practices such as hard drive encryption and data retention limitations?
- **DOCUMENTATION:** Are you maintaining documentation of privacy and security efforts and issues?
- **PRIORITIZATION AND ACTION PLAN:** Have you developed an action plan for achieving compliance based on your gap analysis? Are plans being implemented to address any major risks identified during your analysis?

**YES**

**NO**

**SAFE**

**DANGER!!**