FICHE THÉMATIQUE — NOVEMBRE 2024

CYBERSÉCURITÉ : SGP MICROENTREPRISES & DORA

En plus du principe général de proportionnalité mentionné à l'article 4 de DORA, ce règlement européen précise que certaines exigences sont allégées pour les SGP classées comme microentreprises.

QU'EST-CE QU'UNE MICROENTREPRISE ?

Une entité qui emploie moins de 10 personnes et dont le chiffre d'affaires annuel et/ou le total du bilan annuel n'excède pas 2 millions d'euros.

PAR OÙ COMMENCER ?

- **Cartographiez votre système d'information.** Identifiez et répertoriez les prestataires informatiques de votre SGP et les fonctions supportées par ces prestataires, notamment celles critiques ou importantes dont l'arrêt peut avoir un impact significatif pour l'activité de la SGP.

  Cette première étape vous permettra de détecter les sources de risques spécifiques à votre SGP.

ENSUITE ?

- **Consultez le *Guide pratique DORA***

  Élaboré par le Groupe de travail Cybersécurité de l'AFG, ce guide vous apporte des indications concrètes sur les attentes en termes de conformité et de bonnes pratiques.

- **Pour les SGP microentreprises, le guide met en évidence les points essentiels du Règlement DORA** pour vous aider à anticiper son entrée en vigueur le 17 janvier 2025.
- **Vous y trouverez un contexte de proportionnalité et des exigences adaptées à votre taille**, facilitant la mise en œuvre progressive des dispositions réglementaires.

Le Règlement DORA traite tout particulièrement les services TIC.
Un service TIC (Technologies de l'Information et de la Communication) désigne tout service qui utilise des technologies numériques pour traiter, stocker, transmettre ou recevoir des informations.

QUELLES SONT LES EXIGENCES MINORÉES ?

1. Gestion des risques liés aux TIC

▸ **Gouvernance, organisation et cadre de gestion**

Pour les SGP microentreprises, les exigences en matière de gouvernance et d'organisation des risques liés aux Technologies de l'Information et de la Communication (TIC), peuvent être simplifiées grâce au principe de proportionnalité. Elles ne sont pas obligées de mettre en place des dispositifs plus complexes.

Les stratégies, procédures et outils de gestion des risques TIC doivent être adaptés à la taille et à la portée de leurs activités.

Une revue périodique du cadre de gestion des risques TIC est nécessaire. Toutefois, une revue annuelle n'est pas obligatoire sauf en cas d'incident majeur lié aux TIC.

▸ **Plan de réponse et rétablissement**

Si toutes les SGP doivent avoir des plans de continuité d'activité pour les TIC et des plans de réponse et de rétablissement régulièrement revus, certaines modalités sont allégées pour les microentreprises (article 11).

▸ **Politiques, procédures de sauvegarde, restauration et examens post incident**

Les politiques et procédures de sauvegarde et de restauration et les examens post incidents s'appliquent à toutes les entités financières. En revanche, les SGP microentreprises doivent évaluer, en fonction de leur profil de risque, s'il est nécessaire de maintenir des capacités redondantes en matière de TIC.

2. Catégorisation et notification des incidents majeurs liés aux TIC

Vos (éventuels) incidents devront être classifiés en s'appuyant sur des seuils pour identifier les incidents majeurs liés aux TIC en intégrant la proportionnalité avec un rapport préformaté par les ASEs.

L'article 18-4 précise que les ESAs « tiennent dûment compte de la nécessité pour les microentreprises et les petites et moyennes entreprises de mobiliser des ressources et des capacités suffisantes afin de garantir une gestion rapide des incidents liés aux TIC ».

3. Test de résilience opérationnelle numérique

Dans une démarche basée sur les risques, les SGP microentreprises doivent réaliser des tests de sécurité. Les ressources à consacrer à ces tests doivent être proportionnées :

– au type de risque ;
– à la criticité des actifs informationnels et des services fournis ;
– à tout autre facteur pertinent (article 25.3).

Cependant, l'obligation de réaliser des tests d'intrusion basés sur la menace (TLPT) et de suivre un programme de tests de résilience opérationnelle numérique ne leur est pas applicable.

4. Management des tiers prestataires de services informatiques TIC

Principes

Toutes les entités doivent gérer les prestataires de services informatiques tiers. Néanmoins, les SGP microentreprises ne sont pas tenues d'adopter une stratégie multifournisseurs.

Accords contractuels

Le Règlement DORA précise les mentions obligatoires à inclure dans les contrats passés avec prestataires de services TIC. Lorsqu'une SGP microentreprise est concernée, le prestataire peut stipuler contractuellement que les droits d'accès, d'inspection et d'audit sont délégués à un tiers indépendant désigné par le prestataire.

Les accords contractuels pour les services informatiques soutenant des fonctions critiques ou importantes doivent inclure des mentions supplémentaires. Cependant, selon l'article 30.4 DORA, les autorités publiques devraient fournir des clauses contractuelles types, afin de faciliter la mise en conformité, en particulier pour les SGP microentreprises.

Garder trace de vos échanges avec ces prestataires et notamment de leurs éventuels refus.

Registre

Il n'y a pas de dispositions spécifiques aux SGP microentreprises s'agissant du registre des accords contractuels. L'ensemble des exigences générales relatives à la tenue de ce registre s'appliquent sans exception.

AFG
Ensemble, s'investir pour demain

L'Association Française de la Gestion financière (AFG) représente et promeut l'utilité de la gestion d'actifs pour l'avenir de notre pays. Elle regroupe plus de 440 membres, dont 340 sociétés de gestion, qui gèrent 90 % des encours sous gestion en France.

L'AFG soutient le développement de la gestion d'actifs française au bénéfice des épargnants, des investisseurs et des entreprises.

L'AFG s'investit pour une réglementation stable, efficace et compétitive, avec un engagement fort : permettre aux épargnants de financer leurs projets de vie tout en mobilisant l'épargne privée vers les entreprises qui se transforment.

Publication réalisée par le pôle Expertises et le Groupe de travail Cybersécurité

- Valentine Bonnet, Directrice Gouvernement d'entreprise et Conformité
  T : +33 (0) 44 94 94 00 | v.bonnet@afg.asso.fr

41 rue de la Bienfaisance | 75008 Paris | T : +33 (0)1 44 94 94 00
Avenue de Cortenbergh 100 | 1000 Bruxelles

www.afg.asso.fr