EXPLICATION DES MESURES DE PROTECTION DES DONNÉES

Les informations indiquées ci-dessous seront consultables à l'avenir sur le site internet, dans la rubrique consacrée à la protection des données :

Les mesures techniques et organisationnelles encadrant le traitement des données doivent être indiquées dans le contrat.

La base juridique est le § 11 alinéa 2 BDSG, qui décrit quels tests un Donneur d'ordre doit effectuer avant d'attribuer un contrat. Ainsi, le Preneur d'ordre doit être choisi minutieusement en fonction de la fiabilité et de l'adéquation des mesures techniques et organisationnelles qu'il a prises. Les mesures techniques et organisationnelles doivent notamment être établies par écrit, dans la commande. Le Donneur d'ordre doit également vérifier si les mesures nécessaires conformément à l'annexe au § 9 BDSG ont bien été prises.

Si les données personnelles à traiter contiennent des informations dont le traitement ne devrait pas représenter un risque particulier pour les personnes concernées, le Manuel de sécurité informatique de base du BSI peut servir de catalogue de mesures de sécurité pour une série de questions techniques. (Le manuel dans lequel les mesures sont expliquées peut être commandé auprès du BSI est téléchargé sur un support de données (www.bsi.de).)
Si le Preneur d'ordre dispose d'une politique de protection des données, le Donneur doit vérifier et établir par écrit si cette politique répond à ses exigences. Les objectifs de sécurité sont listés dans l'annexe au § 9 BDSG. Si la politique de sécurité n'est pas suffisante, il s'agit de convenir de mesures supplémentaires. Le système de sécurité qui en résultera devrait faire partie intégrante du contrat. Dans ce cas, il n'est pas nécessaire de répéter les mesures incluses dans le système de sécurité dans le contrat.

Si le Preneur d'ordre ne peut présenter aucune politique de protection des données, les mesures doivent être indiquées dans le contrat. À cet effet, nous rappelons que les objectifs de sécurité à atteindre sont listés dans l'annexe au § 9 BDSG. Chaque mesure du catalogue doit être reprise dans le contrat. Il ne s'agit pas d'un catalogue de mesures final. Des mesures supplémentaires sont généralement nécessaires, notamment en cas de traitement de données sensibles.

Les règles relatives aux éléments suivants sont particulièrement importantes :

- **Responsabilités :** Une distribution floue des tâches, par exemple pour l'attribution des droits d'accès, crée des points faibles dont le risque est considérable.

- **Isolation des réseaux :** Des mesures doivent être prises pour éviter autant que possible toute intrusion non autorisée dans le réseau informatique. En général, une sécurité absolue est impossible, toute tentative d'intrusion devra donc être détectée le plus rapidement possible. Les composants techniques à prendre en compte sont les pare-feux, les systèmes de détection des intrusions et surtout une procédure de cryptage moderne.

- **Interception de communication :** En protection contre toute interception non autorisée des communications, les données doivent être cryptées selon le niveau actuel de technique.

- **Procédures d'inscription :** L'inscription au système ou à l'application représente la première et la plus importante des barrières pour repousser les personnes non autorisées. Des mesures haut de gamme doivent donc être prises dans ce domaine.