Mesures techniques et organisationnelles selon l'art. 32 du RGPD

1. Contrôle d'accès

Le contrôle d'accès doit empêcher que des personnes non autorisées aient accès à des systèmes informatiques de la société 1&1 Internet SARL. Les centres de calcul de la société 1&1 Internet SARL garantissent une protection élevée grâce à une technique de sécurité moderne et des mesures complètes de protection des objets et des données. Cela implique un accès au centre de calcul limité à un cercle restreint de collaborateurs autorisés.

1.1. Mesures organisationnelles

1.1.1. Obligation de réception et d'identification

Le site du bâtiment du centre de calcul est surveillé par un gardien la journée pendant les heures normales d'ouverture et par un service de sécurité en dehors des heures d'ouverture. Toute anomalie est découverte par l'alarme anti-effraction et les rondes du service de sécurité. Tous les visiteurs et collaborateurs extérieurs à l'entreprise doivent porter leur badge sur eux sur le site du centre de calcul. Les personnes extérieures sont en principe autorisées à séjourner au sein du bâtiment uniquement si elles sont accompagnées d'un collaborateur interne à l'entreprise. Les collaborateurs internes à l'entreprise disposent de l'autorisation adéquate pour qu'ils accèdent aux locaux commerciaux grâce à leur carte d'admission correspondante.

La directive relative aux badges prévoit les exigences suivantes pour l'émission des badges :

- les badges, le journal de bord des badges ainsi que tous les documents correspondants doivent être conservés à un emplacement qui peut être verrouillé.
- Les accès aux outils de gestion informatiques doivent être pourvus de mots de passe de façon à ce qu'aucune personne non autorisée ne puisse avoir accès aux postes qui gèrent les badges.
- Les badges doivent être soumis à une date d'expiration.
- La délivrance et la reprise des badges doivent être consignées dans un livre de badges sous forme papier.
- Les inscriptions du livre des badges doivent être conservées pendant au moins 6 mois.
- Chaque « visite » doit être mentionnée sur une feuille de façon à ce que différents visiteurs ne puissent pas avoir connaissance des autres visiteurs s'ils n'ont pas participé à une même visite.

1.1.2. Attribution des clés

Grâce au système de contrôle des entrées installé, seules les personnes qui ont reçu des autorisations au préalable dans le cadre de l'accomplissement de leurs tâches (par ex. opérateurs système devant remplacer le matériel) peuvent pénétrer dans le centre de calcul. Les conditions d'accès sont configurées de façon centralisée par un système de gestion des droits d'accès, c'est-à-dire par la configuration de profils et l'octroi/le blocage d'autorisations. Un processus de validation formel existe à cet effet. Il est possible d'accéder au centre de calcul grâce à une carte

d'accès neutre qui est remise à la personne autorisée sur demande et après signature du destinataire. L'octroi des cartes d'accès est documenté. En cas de perte de la carte d'accès, celle-ci est immédiatement verrouillée depuis le système de gestion installé. Les autorisations peuvent être modifiées, supprimées ou bloquées indépendamment de la disponibilité physique de la carte d'accès.

1.2. Mesures techniques

Le centre de calcul est protégé d'un accès non autorisé grâce aux mesures techniques suivantes :

- Système de contrôle des entrées
- Alarme anti-effraction homologuée VdS1
- Caméras
- Portes de sécurité
- Contrôle de changement de zone

Un composant important du concept de sécurité est l'accès au centre de calcul par le biais d'une installation d'accès individuel.

1.2.1. Dispositif de sécurité pour la porte

Un sas de sécurité garantit que les personnes autorisées accèdent au centre de calcul une par une. L'accès au sas de sécurité requiert une clé électronique (dite support d'identification informatisé) avec code PIN qui doit être explicitement activée pour l'accès. L'accès au centre de calcul à travers le sas de sécurité est uniquement accordé si le contrôle des dispositifs de sécurité rend un résultat positif.

1.2.2. Système de contrôle des entrées et surveillance

Le site du centre de calcul dispose de lecteurs d'accès sur toutes les portes extérieures ainsi que de lecteurs sur les barrières. Tous les accès extérieurs, portes d'étage et espaces de bureau sont équipés de cylindres de fermeture numériques. Tous les accès au centre de calcul sont sous surveillance vidéo grâce à un système de surveillance centralisé. Les enregistrements sont conservés pour une période de 6 mois. Les portes des issues de secours sur le site du centre de calcul sont équipées en outre d'une commande des portes des issues de secours qui est planifiée, certifiée et entretenue régulièrement selon les prescriptions du VdS.

2. Contrôle d'accès

Le contrôle d'accès doit empêcher toute personne non autorisée d'accéder aux systèmes informatiques de la société 1&1 Internet SARL. Des mesures techniques et organisationnelles relatives à l'identification et à l'authentification de l'utilisateur sont mises en œuvre à cet effet.

2.1. Mesures organisationnelles

2.1.1. Procédure pour utilisateurs et autorisations

Les utilisateurs devant obtenir des droits d'accès à un système dans le cadre de l'accomplissement de leurs tâches doivent demander ces autorisations par le biais d'une procédure pour utilisateurs et autorisations formelle. Les exigences posées à l'affectation de

l'utilisateur et de l'autorisation sont décrites dans la directive de sécurité interne relative à la gestion des identités et des accès, et l'affectation des autorisations est documentée dans des instructions relatives à la procédure. Les identifiants et les autorisations des utilisateurs figurent dans le système de gestion des utilisateurs et des autorisations. Des systèmes de tickets documentant la procédure permettent de gérer du point de vue technique la validation de délivrance et de suppression des droits d'accès. Dans le système de gestion, les autorisations des utilisateurs sont bloquées dès que l'utilisateur quitte l'entreprise ou lorsque les autorisations ne sont plus nécessaires ou sont utilisées de manière non autorisée. Des droits d'accès obsolètes sont également supprimés dans le cadre de ce diagnostic de système. Grâce à un procédé technique, chaque utilisateur autorisé dispose d'un seul identifiant d'utilisateur sur le système cible.

2.2. Mesures techniques

2.2.1. Procédure d'authentification

Les droits d'accès sont configurés aussi précisément que possible de façon à ce que les personnes aient seulement accès là où elles en ont besoin de par leur fonction et l'accomplissement de leurs tâches. Les procédures de contrôle d'accès sont valables pour tous les collaborateurs de la société 1&1 Internet SARL. Tous les systèmes sont protégés par une procédure d'authentification à deux niveaux (par ex. identifiant utilisateur et mot de passe) qui empêche les accès non autorisés. Si, dans le cadre, de la procédure d'authentification, des mots de passe sont utilisés, ils doivent alors satisfaire aux directives relatives aux mots de passe pour les collaborateurs et systèmes. Les mots de passe, qui ne satisfont pas à la qualité exigée par les directives, ne sont pas autorisés. Les systèmes sont automatiquement verrouillées après un temps défini d'inactivité. En outre, les comptes sont automatiquement désactivés si les mots de passe correspondants ne sont pas modifiés.

Un accès à distance aux systèmes internes n'est possible que sous la forme d'une authentification pour laquelle sont utilisées des procédures d'authentification asymétriques (procédure de clés publique/privée) qui sont en outre enregistrées pour la détectabilité. L'accès à des systèmes internes n'est accordé aux seuls appareils qui se trouvent en possession de la société 1&1 Internet SARL et qui sont administrés. L'accès aux systèmes internes par le biais d'une connexion sans fil n'est possible qu'à travers un tunnel VPN supplémentaire. Les dispositifs d'accès au réseau Wi-Fi exploités par la société 1&1 Internet SARL détectent et enregistrent les points d'accès non autorisés.

2.2.2. Chiffrement

Les données qui requièrent un niveau de protection élevé sont sauvegardées conformément au niveau actuel de la technique avec une procédure chiffrée analogique à la directive sur la sécurité informatique interne relative à la cryptographie. Les procédés de cryptage utilisés sont basés sur les recommandations de l'Office fédéral de la Sécurité des technologies de l'information (BSI). Si des données sont échangées à l'aide d'un support de données, les informations relatives à l'échange sont consignées : personne ayant reçu le support de données, date et heure de la remise, but de l'échange et personne ayant remis le support de données. Les supports de données qui ne sont plus utilisés de façon productive sont éliminés grâce à une procédure de suppression et de réécriture sûre conforme aux recommandations du BSI. Les dispositions de la directive sur la sécurité interne relative à l'élimination des médias s'appliquent ici.

3. Contrôle d'accès

Le contrôle d'accès permet d'empêcher des actes illicites dans les systèmes informatiques de la société 1&1 Internet SARL en mettant en œuvre des mesures de surveillance et de procès-verbaux des accès.

3.1. Affectation d'autorisation

Les systèmes ont été configurés de façon à ce qu'un accès régulier avec les droits administratifs soit possible uniquement pour les collaborateurs internes autorisés issus de segments de réseau sûrs. Des concepts d'autorisation répondant aux besoins et définissant les droits d'accès ainsi que leur surveillance et leur archivage ont été développés ici. Une attribution d'autorisation est toujours affectée selon le principe du besoin d'en connaître. Selon les droits, différentes autorisations sont configurées en étant divisées en rôles et profils d'utilisateurs. D'autres autorisations aux systèmes requièrent la configuration d'autorisations selon le processus d'utilisateur et d'autorisation mis en œuvre.

3.2. Analyses

Les accès aux identifiants du système et tentatives d'accès évidentes sont archivés dans un serveur d'archivage centralisé. L'accès au serveur d'archivage n'est possible qu'en lecture aux administrateurs autorisés. En cas d'essai d'accès évident, une alarme (surveillance de sécurité) est déclenchée permettant de prévenir le responsable du système.

3.3. Modifications

Des modifications des droits d'accès ne peuvent être réalisés que par les administrateurs du système du domaine opérationnel qui ont reçu la validation de leurs supérieurs. Les droits d'accès et les autorisations sont modifiés en règle générale dans un délai d'un jour ouvrable ou immédiatement si nécessaire. Les périphériques réseau ou les systèmes avec possibilités d'accès prédéfinies ne doivent pas être utilisés dans le domaine productif. Les directives de sécurité internes réglementent les points restants.

3.4. Suppression

La suppression des autorisations d'utilisateur (par ex. après le départ d'un collaborateur) est réalisée rapidement, au plus tard toutefois dans un délai d'un jour ouvrable. La suppression des droits d'accès est également réalisée dans le cadre du diagnostic de système. Des droits d'accès obsolètes sont également supprimés dans ce contexte. Dans le système de gestion, les autorisations des utilisateurs sont bloquées dès que l'utilisateur quitte l'entreprise ou lorsque les autorisations ne sont plus nécessaires ou sont utilisées de manière non autorisée. Des droits d'accès obsolètes, qui n'ont par ex. pas été activés pendant une période prolongée, sont également supprimés dans le cadre du diagnostic de système.

4. Contrôle de transmission

Dans le cadre du contrôle de transmission, des mesures sont définies lors du transport, de la transmission et du transfert ainsi que lors du contrôle ultérieur des données à caractère personnel.

4.1. Mesures organisationnelles

4.1.1. Mesures de formation

Tous les collaborateurs de la société 1&1 Internet SARL sont soumis à une obligation de confidentialité. Les nouveaux collaborateurs reçoivent une formation en sécurité au moment de leur entrée dans l'entreprise. Pour différents domaines, des programmes de sensibilisation à la sécurité spécialement adaptés sont proposés.

4.1.2. Classification des informations

Chaque information doit être classée selon son besoin de protection. S'il s'agit d'informations confidentielles, elles doivent être traitées de façon particulière. Les informations confidentielles et de service ne doivent être transférées que par le biais de voies de communication sûres. Le traitement des informations a été réglementé dans la directive « Classification des données » et son annexe. Les règles suivantes doivent être tout particulièrement respectées :

- des procédés spéciaux et des règles spécifiques doivent être définis et documentés pour la protection des informations et des supports de données lors du transport, en particulier, au-delà des limites de l'entreprise (par ex. instruction de procédure pour l'utilisation de coursiers).
- Dans la mesure du possible, des procédures cryptographiques (par ex. chiffrement lors du transfert de données confidentielles) doivent être mises en œuvre. Les exigences de la directive sur la sécurité informatique et la cryptographie doivent être respectées.
- Lors du transfert à des destinataires externes, le transfert réalisé, complet et sûr doit être documenté et la preuve doit en être donnée.

4.2. Mesures techniques

4.2.1. Sécurisation d'accès et sécurité de transport

Seuls les utilisateurs autorisés peuvent par principe accéder aux systèmes qui traitent des données à caractère personnel. Les données sont transférées exclusivement par le système lui-même à des destinataires autorisés par des voies fortement sécurisées par la cryptographie par ex. via VPN avec IPSec conformément au niveau actuel de la technique et aux recommandations du BSI. Le transfert est archivé dans des fichiers journaux.

Afin de protéger le système des accès non autorisés d'ordinateurs de bureau des collaborateurs et ainsi du transfert de données non autorisé, les directives internes sur la sécurité s'appliquent pour les collaborateurs de la société 1&1 Internet SARL.

L'intégrité des fichiers importants du système est assurée grâce à un contrôle régulier de leur total de contrôle cryptographique (HIDS).

La protection des accès aux systèmes contenant des informations sensibles est réalisée sur plusieurs niveaux : au niveau du système de fichiers, du système d'exploitation et au niveau du réseau. Les mécanismes de protection permettent seulement aux administrateurs spécialement

autorisés l'accès au niveau correspondant. Toutes les données en relation avec le travail doivent être enregistrées sur les serveurs afin d'éviter une perte des données. Ces données sont régulièrement enregistrées conformément aux concepts de sauvegarde définis de façon à ce qu'une perte de données soit ainsi exclue en grande partie.

4.2.2. Archivage

L'accès et les activités des administrateurs sont enregistrés dans des fichiers journaux spéciaux. Les accès sont enregistrés sur un serveur d'archivage centralisé, dédié qui est installé en étant séparé des systèmes à archiver. L'accès aux protocoles et au serveur d'archivage central est protégé et n'est possible qu'aux administrateurs autorisés. Les administrateurs du système ne peuvent ce faisant que voir les protocoles sur le serveur d'archivage mais ne peuvent pas les modifier. Les données d'archivage sont transportées via une connexion cryptée. Différentes violations des contrôles de sécurité telles que des tentatives d'accès non autorisées ou des violations de protection significatives sont enregistrées sur le serveur d'archivage. En cas de systèmes particulièrement sensibles, l'accès n'est possible qu'en fonction du principe des quatre yeux.

5. Contrôle d'entrée

Pour assurer la transparence et la documentation de la gestion des données, des mesures de contrôle ultérieur sont mises en œuvre afin de savoir si des données ont été saisies, modifiées ou supprimées et qui s'en est chargé.

5.1. Analyse de l'archivage et du protocole

Grâce au respect des règles sus-mentionnées relatives au contrôle des entrées et au contrôle des accès, la base du contrôle de saisie des systèmes, qui traite les données, est créée. Dans le concept des droits et des rôles, il est différencié entre les utilisateurs du système, les utilisateurs du processus et les utilisateurs personnalisés.

Des indications relatives à l'archivage figurent dans le chapitre 4.2.2.

Les protocoles sont analysés de manière aléatoire par les administrateurs du système, en particulier toutefois lorsque des anomalies ou une suspicion de compromission (par ex. en raison d'une alarme / du déclenchement d'un événement) sont intervenues. Les analyses de protocole sont classées comme informations qui ne doivent être utilisées qu'au sein de la société 1&1 Internet SARL afin de maintenir et d'assurer la stabilité et la sécurité du système.

6. Contrôle des mandats

Toutes les instructions du donneur d'ordre relatives au traitement des données à caractère personnel sont documentées et déposées au point central pour les collaborateurs chargés du traitement des données de la société 1&1 Internet SARL.

La société 1&1 Internet SARL traite les données personnelles exclusivement dans le cadre des conventions conclues. Le but, le type et l'étendue du traitement des données sont exclusivement basés sur les instructions du donneur d'ordre. Un traitement en divergeant ne peut avoir lieu

qu'après accord écrit du donneur d'ordre. La personne chargée de la protection des données par le donneur d'ordre a le droit de contrôler à tout moment après accord la mise en œuvre de ses instructions dans la société 1&1 Internet SARL. La société 1&1 Internet SARL assistera le donneur d'ordre lors de la réalisation des contrôles par le donneur d'ordre et participera au déroulement intégral du contrôle.

La société 1&1 Internet SARL informera immédiatement le donneur d'ordre si une instruction donnée par le donneur d'ordre contrevient selon elle aux dispositions légales et règlementations et communiquera au donneur d'ordre dans les plus brefs délais tout non-respect des prescriptions relatives au droit concernant la protection des données ou des conventions contractuelles conclues et/ou des instructions délivrées par le donneur d'ordre, intervenu dans le cadre du traitement des données assuré par ses soins ou autres personnes chargées du traitement. La société 1&1 Internet SARL est tenue de garder confidentielles les données lors du traitement des données pour le donneur d'ordre. Elle s'engage à respecter les mêmes règles en matière de protection des secrets, telles qu'elles incombent au donneur d'ordre. Les documents qui ne sont plus nécessaires et qui comportent des données et des fichiers à caractère personnel seront détruits en respectant la protection des données uniquement après accord préalable du donneur d'ordre.

7. Contrôle de disponibilité

Tous les services de la société 1&1 Internet SARL et de ses filiales sont très sensibles en ce qui concerne leur disponibilité et doivent être protégés de toute destruction ou perte accidentelle. Les clients attendent une fourniture hautement disponible de toutes les prestations de réseau et du centre de calcul. Dans ce contexte, des mesures de sauvegarde et de maintien des données sont mises en œuvre.

7.1. Mesures organisationnelles

7.1.1. Manuels de secours et procédure de sauvegarde

Pour assurer les manuels de secours et les procédures de sauvegarde, des manuels de secours sont rédigés dans les services pour lesquels cela est jugé nécessaire. Les manuels de secours définissent les responsabilités (par ex. la personne responsable en cas d'urgence) ainsi que les chemins de remontée, d'information et d'alarme, déterminent les plans de redémarrage et procédures pour un arrêt en cas de défaut, règlent l'achat de remplacement du matériel et du logiciel et documentent la façon dont les données sont sauvegardées et archivées. Les manuels de secours représentent ainsi un élément essentiel du traitement et de la manipulation des systèmes et données en cas d'urgence qui renvoient tout particulièrement à des stratégies et des documentations de sauvegarde. Toutes les données sont enregistrées à intervalles réguliers, la sauvegarde étant documentée à un autre emplacement que là où est conservé le système à sauvegarder. Les sauvegardes ne quittent toutefois pas le centre de calcul de la société 1&1 Internet SARL. Pour protéger les archives et sauvegardes, les contrôles d'accès susmentionnés sont mis en œuvre. L'accès au logiciel de sauvegarde est limité aux administrateurs de sauvegarde dédiés. La fréquence des sauvegardes des données dépend de la criticité des informations et peut être ajustée individuellement. Des tests de fonctionnalité des sauvegardes de données sont réalisés de manière aléatoire par les administrateurs responsables du système.

Les supports de stockage utilisés pour la sauvegarde sont réutilisés après une procédure sûre de suppression ou de réécriture conformément à la recommandation du BSI.

Dans le processus de restauration, il est décrit la façon dont les systèmes et les données doivent être installés et restaurés et dans quel ordre.

Tous les processus de restauration des données, le plan de redémarrage des systèmes ainsi que la situation d'urgence doivent être réalisés et testés à intervalles réguliers au cours d'un exercice. Les tests et exercices sont enregistrés et documentés. Les chemins de remontée requis en cas d'urgence et d'incidents ont été éprouvés dans la pratique.

7.2. Mesures techniques

7.2.1. Pare-feu et protection antivirus

Les réseaux et systèmes de la société 1&1 Internet SARL, qui sont entretenus et actualisés régulièrement par des administrateurs de système autorisés, sont protégés avec un pare-feu contre les piratages informatiques. Les règles du pare-feu sont énoncées de telle façon que seuls les services requis sont autorisés et bloquent tout trafic réseau dans le réglage de base. Toutes les connexions Internet sont protégées par un pare-feu au moins. Le contrôle des configurations relatives à la sécurité est réalisé à cet effet dans le cadre d'audits de sécurité et de tests d'intrusion qui sont réalisés entre autres par le service de sécurité. Tous les composants de réseau sont contrôlés une fois par jour, aussi bien de manière interne qu'externe grâce à des scanners automatiques.

Le concept de protection antivirus prévoit une protection à plusieurs niveaux contre le logiciel malveillant via les passerelles de réseau et les systèmes de la société 1&1 Internet SARL. La protection contre le logiciel malveillant est gérée de façon centralisée grâce à un système de gestion des systèmes et actualisée régulièrement, au moins une fois par jour. Tous les systèmes sensibles et critiques sont équipés d'un ensemble de disques durs à tolérance de pannes (en règle général RAID 5).

7.2.2. Haute disponibilité et alimentation électrique

Pour répondre aux exigences de haute disponibilité, le site de Karlsruhe, où le système est installé, présente comme base une infrastructure de réseau hautement redondante capable de parer aux fautes isolées dans pratiquement tous les domaines et aux fautes doubles dans de nombreux domaines. Les services critiques sont exploités sur différents sites (géo-redondan©. L'alimentation électrique est constituée de plusieurs sources indépendantes les unes des autres. Le centre de calcul est équipé d'une alimentation électrique ininterrompue. La technologie électrique centrale du centre de calcul principal de Karlsruhe est divisée en quatre blocs (3+1). Chaque bloc inclut des lignes de moyenne tension, de basse tension, d'ASI et une installation auxiliaire d'alimentation. Un bloc de service sert d'installation redondante.

Les blocs d'alimentation sont géographiquement séparés les uns des autres afin d'empêcher une influence réciproque en cas de dommage ou de panne. Chaque bloc a sa propre sortie côté moyenne tension. Le centre de calcul est raccordé à un réseau de 20 kV des services publics municipaux de Karlsruhe qui est exclusivement réservé au centre de calcul. Afin de se protéger d'une défaillance complète de l'alimentation fournies par les services publics municipaux, une alimentation sans interruption (ASI) redondante est installée en second lieu entre le consommateur et le fournisseur. L'ensemble de l'installation est surveillée et contrôlée grâce à

un système de contrôle du réseau redondant. En outre, la qualité de réseau de toutes les entrées et sorties des installations ASI est surveillée en permanence conformément à la norme DIN EN 50160.

7.2.3. Protection incendie

Un installation d'extinction d'incendie à l'argon protège les locaux de sécurité en cas d'incendie. Le gaz non toxique entraîne, en cas d'incendie, un déplacement de l'oxygène dans le local, ce qui permet de retirer l'élément de base oxygène à la source de feu. Les serveurs ne sont pas affectés par la procédure d'extinction et peuvent être encore normalement exploités.

Afin d'empêcher un incendie en amont, une installation de détection précoce d'incendie, qui surveille en permanence les particules dans l'air au moyen d'une période de calibrage de consigne prédéfinie, est installée en outre. Si la composition des particules dans l'air change ou si le nombre de particules typiques pour la survenance d'un incendie augmente, la détection précoce donne l'alarme. L'installation est directement connectée à la centrale des sapeurs-pompiers professionnels de Karlsruhe. Une commande de notification, un email ou l'envoi d'un SMS à la gestion des équipements de la société 1&1 Internet SARL à Karlsruhe permet de localiser l'alarme au sein du système. L'installation a été planifiée et certifiée d'après les prescriptions de VdS. Des détecteurs d'incendie sont installés dans tous les locaux de la domotique, dans toutes les pièces techniques, les entrepôts, les corridors et les cages d'escaliers et des déclencheurs manuels d'alarme sont installés dans toutes les zones d'accès. Le système d'alarme est entretenu régulièrement conformément aux prescriptions de VdS. Des extincteurs portables sont installés pour les premières mesures de lutte contre l'incendie.

8. Contrôle de la séparation

Les mesures prises par la société 1&1 Internet SARL pour le contrôle de la séparation sont la connexion logicielle au sens d'une séparation des clients, la séparation des programmes de test et de routine, la séparation par l'application de règlements d'accès ainsi que la séparation des fichiers.

Tous les systèmes productifs doivent être notamment exploités séparément des systèmes de développement et de test. Cette séparation est réalisée du point de vue technique grâce à une segmentation des réseaux à l'aide d'un ensemble de règles pare-feu activées. Les données productives ne doivent pas être utilisées comme copies à des fins de test et, de la même manière, les données de test ne doivent pas être utilisées dans l'environnement productif. Pour le détail, voir les directives de sécurité internes pour une exploitation sûre.