Check-list relative à la nouvelle loi sur la protection des données

La check-list suivante offre une vue d'ensemble des principales mesures devant être prises par les clubs avant l'entrée en vigueur de la nouvelle loi sur la protection des données le 1er septembre 2023. Elle contient deux catégories de tâches: celles qui sont prescrites par la loi et celles qui sont recommandées.

	Obligatoire	Recommandé
Stratégie en matière de protection des données		Il est recommandé d'établir avant le 1er septembre 2023 un **plan de *compliance*** incluant l'élaboration des documents, des processus, etc. nécessaires ainsi que les responsabilités, les objectifs et les échéances.
Registre des activités de traitement	Les responsables de structures employant **250 personnes** ou plus doivent établir un registre récapitulant l'ensemble des traitements de données et l'actualiser régulièrement. Cette obligation s'applique quel que soit le nombre de personnes employées en cas de **traitement de données sensibles à grande échelle** ou de **profilage à risque élevé**.	Il est recommandé de dresser un **inventaire du traitement des données** même si l'établissement d'un tel registre n'est pas obligatoire car, pour chaque projet touchant à la conformité à la protection des données, on doit définir dans un premier temps quelles sont les données traitées, comment elles le sont et pourquoi.
Gestion des risques liés à la protection des données	Il faut procéder à une **analyse d'impact relative à la protection des données personnelles** dès lors qu'un traitement de données est susceptible d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée. Cela implique de définir des **processus afin d'évaluer les risques** et de **réaliser une telle analyse.**	

	Obligatoire	Recommandé
Devoir d'information des personnes concernées	Lors de la collecte de données personnelles, la personne concernée doit être **informée du traitement de données prévu**. Il faut alors lui communiquer les informations nécessaires pour qu'elle puisse faire valoir ses droits et pour que la transparence du traitement des données soit garantie.	Bien que ces informations ne doivent pas impérativement être transmises par écrit, il est fortement recommandé de le faire pour des raisons pratiques et liées à la fourniture de preuves. L'élaboration de **déclarations de protection des données** () suffit généralement à satisfaire à ce devoir d'information: p. ex. dans le cadre de l'adhésion au club, sur le site Internet et vis-à-vis du personnel.
Règlements et directives internes	Dans certaines circonstances, il est obligatoire de **documenter** les traitements de données et d'élaborer un **règlement en la matière**, notamment en cas de traitement automatisé de données sensibles à grande échelle ou de profilage à risque élevé.	Parallèlement à ces obligations éventuelles, il est recommandé de rédiger des **directives internes** garantissant le respect des règles en matière de protection des données et contenant des **instructions** à l'attention des fonctionnaires de club et du personnel en lien avec la protection des données personnelles et la sécurité des informations. Ce document peut également définir les **responsabilités et rôles** internes dans le domaine de la protection des données.
Traitement de données par des tiers	En cas d'**externalisation de traitements de données à des tiers** (p. ex. à une entreprise informatique chargée d'héberger le site Internet du club et ayant donc accès à des données personnelles), il convient de s'assurer que **le traitement des données personnelles par ces tiers se limite à ce que le responsable du traitement aurait fait lui-même** et qu'ils garantissent la **sécurité des informations**.	Pour des raisons pratiques et liées à la fourniture de preuves, il est recommandé de conclure **un contrat écrit de sous-traitance du traitement de données** définissant notamment les droits et devoirs du responsable du traitement ainsi que du sous-traitant.

	Obligatoire	Recommandé
Réglementation relative aux obligations de conservation et d'effacement de données	Conformément au principe de **finalité**, des données personnelles ne peuvent être traitées que dans le but indiqué lors de leur collecte, prescrit par la loi ou résultant des circonstances. Par conséquent, les **données doivent en principe être supprimées une fois le but atteint** (p. ex. en cas de départ d'un membre du club), hormis si un **délai de conservation** plus long (p. ex. 10 ans pour les pièces comptables) est imposé ou si un autre motif le justifie.	Il est recommandé d'élaborer un **règlement interne** précisant les obligations en matière de conservation et d'effacement de données personnelles. Celui-ci peut aussi être intégré aux directives internes susmentionnées.
Sécurité des données	Le responsable du traitement doit assurer, par des **mesures techniques et organisationnelles** appropriées, une sécurité adéquate des données personnelles par rapport au risque encouru.	Il est recommandé de **consigner ces mesures par écrit**.
	Le PFPDT doit être informé aussi rapidement que possible de tout **incident lié à la sécurité des données** (p. ex. si des données personnelles sont involontairement communiquées à des personnes non autorisées ou rendues accessibles à celles-ci) et présentant un risque élevé. Il convient d'informer également la personne concernée, dans la mesure où cela s'avère nécessaire à sa protection.	Le cas échéant, il est recommandé de définir **par écrit un processus** (incluant des instructions et des responsabilités) relatif à l'évaluation du risque d'incident et à l'information éventuelle du PFPDT ainsi que de la personne concernée.

	Obligatoire	Recommandé
Droits des personnes concernées	**Droit d'accès:** toute personne concernée peut demander si des données personnelles à son sujet sont traitées. Le club doit donc être en mesure de la renseigner.	Le cas échéant, il est recommandé de définir **par écrit un processus** (incluant des instructions et des responsabilités) relatif au traitement de telles demandes. Conformément au principe d'exactitude, il est en outre recommandé de définir un processus de **contrôle régulier** des données personnelles traitées par le club.
	Droit de rectification: toute personne concernée peut demander la rectification de données personnelles inexactes. Le club doit donc être en mesure de les corriger.	
	Portabilité des données: toute personne concernée peut demander au responsable du traitement qu'il lui remette les données personnelles à son sujet qu'elle lui a communiquées et qu'il a traitées de manière automatisée. Le club doit donc être en mesure de lui remettre ces informations sous un format électronique couramment utilisé ou, sur demande, de les transmettre à un autre responsable du traitement.	
Transmission de données à l'étranger	En cas de **transmission de données à l'étranger**, le responsable du traitement doit garantir la protection des données, y compris si l'entité chargée du traitement **a accès depuis l'étranger aux données personnelles** du club. En cas de transmission de données vers un pays (p. ex. les États-Unis) n'offrant pas un **niveau de protection adéquat**, notamment, il convient de prévoir des **garanties** supplémentaires (p. ex. des clauses standard de protection des données) et de réaliser une **analyse d'impact relative au transfert des données** avant leur transmission.	Il est recommandé de consigner **par écrit** le processus (incluant des instructions et des responsabilités) relatif à l'évaluation du pays en question et à l'introduction de garanties et mesures supplémentaires éventuellement nécessaires.

	Obligatoire	Recommandé
Sensibilisation et formation à la protection des données		La mise en œuvre et le respect des dispositions relatives à la protection des données ainsi que des directives internes requièrent une sensibilisation adéquate au sein du club. Il est donc recommandé de mener régulièrement des **formations relatives à la protection des données**.
Conseil en matière de protection des données		La nomination d'un **conseiller ou d'une conseillère (interne ou externe) à la protection des données** ainsi que la communication de ses coordonnées au PFPDT ne sont pas impératives, mais peuvent s'avérer pertinentes.
Réexamen régulier des mesures relevant du droit de la protection des données		Il est recommandé de **contrôler** et d'**actualiser régulièrement** les mesures relevant du droit de la protection des données et de **s'assurer de leur respect**.