لمحة عامة عن دليل وابيس لأفضل الممارسات

ينقسم هذا الدليل إلى 12 فصلا.

يقدم الفصل الأول نظرة عامة عن المصطلحات المستخدمة في الدليل. وهو يعرّف خصوصا المصطلحات المتصلة بأبرز الهيئات المسؤولة عن حماية البيانات الشخصية في إطار الدليل (الفصل 1، الفقرتان 1 و2)، ومتلقّي البيانات الشخصية (الفصل 1، الفقرة 8)، والأشخاص الذين تعامَل بياناتهم الشخصية (الفصل 1، الفقرة 4)، ونوع المعلومات التي تُعتبر بيانات شخصية (الفصل 1، الفقرة 7).

ويعرض الفصل الثاني المبادئ العامة التي تحكم حماية البيانات الشخصية والأسباب المشروعة التي لدى أجهزة إنفاذ القانون لمعاملة هذه البيانات. وتوفر هذه المبادئ لهذه الأجهزة إيضاحات عامة لمختلف شروط معاملتها في منظومة وابيس. ومبادئ حماية البيانات الشخصية المعروضة تتصل بما يلي: (a) الموافقة والمشروعية؛ و(b) الشرعية والإنصاف؛ و(c) الغرض والملاءمة والحفظ؛ و(d) الدقة؛ و(e) الشفافية؛ و(f) السرية والأمن؛ و(g) اختيار معامِل البيانات. ولا ينبغي لأجهزة إنفاذ القانون معاملة البيانات في منظومة وابيس إلا لأغراض إنفاذ القانون المشروعة التالية: منع ارتكاب الجرائم أو التحقيق فيها أو الكشف عنها أو مقاضاة مرتكبيها، وتنفيذ العقوبات، وصون النظام العام، وحماية الأمن العام من الأخطار التي تتهدده ومنعها، ولأداء أجهزة إنفاذ القانون أي مهمة أو مسؤولية يمليها عليها القانون.

ويبحث الفصل الثالث دور هيئات حماية البيانات، وأهمية التدريب على كيفية حماية هذه البيانات، وأهمية إشراك أصحاب المصلحة الرئيسيين في تنفيذ إطار حماية البيانات. فأولا، ينبغي لجميع البلدان المشاركة في منظومة وابيس إنشاء هيئة مستقلة لحماية البيانات تكون مسؤولة عن عمليات معاملة البيانات. وثانيا، ينبغي لأجهزة إنفاذ القانون تعيين موظف معني بحماية البيانات ليقوم بما يلي: (a) إطلاع أجهزة إنفاذ القانون على واجباتها القانونية؛ و(b) التحقق من مدى التقيد بشروط معاملة البيانات؛ و(c) تقديم المشورة بشأن تقييم نتائج حماية البيانات؛ و(d) التنسيق مع هيئات حماية البيانات؛ و(e) تنظيم برنامج تدريب مناسب ودائم لمستخدمي منظومة وابيس. وثالثا، يتعين على أجهزة إنفاذ القانون دمج حماية البيانات في صلب هيكليات إدارتها عبر إشراك أصحاب المصلحة الرئيسيين في تنفيذ إطار حماية البيانات التي تعامَل في هذه المنظومة.