2. في حال الاطلاع على بيانات شخصية أو الكشف عنها، ينبغي أن تتيح ملفات العمليات ذات الصلة تبيان الدافع وراء هاتين العمليتين وتاريخ ووقت إجرائهما وتحديد هوية الشخص الذي اطلع على هذه البيانات أو كشف عنها وهوية الشخص الذي تلقّاها.

3. لا ينبغي استخدام ملفات العمليات إلا للتحقق من مدى قانونية المعاملة وللمراقبة الذاتية وكفالة سلامة وأمن البيانات الشخصية وللإجراءات الجنائية. وينبغي لأجهزة إنفاذ القانون وضع هذه الملفات بتصرف هيئة حماية البيانات عند الطلب.

4. لا ينبغي أن يقيّم ملفات العمليات إلا شخص يضطلع بدور "المدقق" المعتمد في المنظومة، وذلك عن طريق هذه المنظومة لا غير.

5. يمكن تعديل الملفات أو حذفها وفقا للسياسات و/أو أفضل الممارسات المقبولة.

7.3 الاحتفاظ بالبيانات

1. ينبغي لأجهزة إنفاذ القانون وضع قواعد و/أو توصيات داخلية تحدد فترة الاحتفاظ بالبيانات الشخصية أو تنص على مراجعة دورية لمدى الحاجة إلى تخزين هذه البيانات.

2. ينبغي لأجهزة إنفاذ القانون أن تراجع دوريا أسباب الاحتفاظ بالبيانات الشخصية ومعاملتها.

3. لتحديد الفترة المناسبة للاحتفاظ بالبيانات الشخصية في المنظومة، ينبغي لأجهزة إنفاذ القانون:
   a. مراجعة طول فترة الاحتفاظ بالبيانات الشخصية استنادا إلى التشريعات الوطنية السارية وطبيعة البيانات والسياسات التي تتبعها وأفضل الممارسات؛
   b. النظر في الغرض المحدد للمعلومات قبل أن تقرر ما إذا كانت ستحتفظ بالبيانات الشخصية (وإلى متى)؛
   c. القيام بشكل مأمون بحذف المعلومات التي لم تعد ضرورية للأغراض المحددة؛
   d. تحديث المعلومات أو وضعها في المحفوظات أو حذفها بشكل مأمون إذا أصبحت قديمة.

4. لا ينبغي الاحتفاظ بالبيانات التي تعامَل في المنظومة إلا للفترة التي تحتاج إليها أجهزة إنفاذ القانون المعنية لتحقيق الغرض منها.