سياسية حماية البيانات الشخصية

التوقيع	التغييرات	المنصب	وافق عليه	الكاتب	التاريخ	النسخة
	الإصدار الاول	الرئيس التنفيذي	هديل العمري	أمير حسن	07/11/2024	1.0.0
	الإصدار الاول	رئيس مجلس الإدارة	عدنان العمري	أمير حسن	07/11/2024	1.0.0

جدول المحتويات

1. المقدمة

يتمثل هدف هذه السياسة في توضيح كيفية تعامل جهة التحكم مع البيانات الشخصية التي تجمعها، وتوفير إرشادات وإجراءات لضمان حماية تلك البيانات وفقا لأفضل المعايير والقوانين الوطنية، تسعى الشركة الى تعزيز الشفافية والمسؤولية في إدارة البيانات الشخصية، بما يحقق الثقة بين الشركة والافراد الذين تقدم لهم خدماتها.

2. نطاق التطبيق:

تنطبق هذه السياسة على جميع البيانات الشخصية التي تجمعها جهة التحكم او الأطراف المتعاقدة معها، وتشمل جميع الموظفين، والمتعاقدين، والشركاء الخارجين الذين يتعاملون مع البيانات الشخصية.

3. التعريفات الأساسية

أ- **جهة التحكم:** هي الجهة التي تحدد اهداف معالجة البيانات الشخصية وطريقة معالجتها. في هذه الحالة، الشركة هي جهة التحكم التي تتحمل مسؤولية جمع، ومعالجة، وحماية البيانات الشخصية.

ب- **البيانات الشخصية:** البيانات الشخصية تعني أي معلومات تتعلق بشخص طبيعي يمكن من خلاله التعرف عليه بشكل مباشر او غير مباشر، مثل الاسم، ورقم الهوية، والعنوان، والبريد الالكتروني، وغيرها.

ج- **البيانات العامة:** هذه البيانات متاحة للجمهور ولا تتطلب اذونات للوصول اليها، عادةً ما تكون هذه البيانات غير حساسة.

د- **البيانات المقيدة:** البيانات التي تتطلب الوصول اليها وجود ضوابط محددة، ولكن لا تحتوي على حساسية عالية.

ه- **البيانات السرية:** البيانات التي تتسم بحساسية كبيرة ويجب حمايتها من الوصول الغير مصرح به.

و- **البيانات الحساسة:** هي البيانات التي تحتوي على معلومات شخصية او سرية ويؤدي كشفها الى انتهاك الخصوصية او الاضرار بالفرد او الكيان.

ز- **البيانات الحرجة:** تشمل البيانات التي يؤدي افشاؤها او التلاعب بها الى تأثير.

ك- **البيانات الائتمانية:** هي معلومات مالية وشخصية تتعلق ببيانات وتاريخ التعاملات الائتمانية للفرد او المؤسسة.

ل- **البيانات الصحية:** المعلومات المتعلقة بصحة الفرد والتي تتضمن أي معلومات تتعلق بحالته الصحية، تشخيصاته، العلاجات التي يتلقاها، او سجلاته الطبية بشكل عام.

4. المبادئ الأساسية لحماية البيانات الشخصية

أ- الشفافية: جمع البيانات الشخصية ومعالجتها يتم بشكل قانوني وشفاف وفقاً للقوانين واللوائح المعمول بها.

ب- التقليل من البيانات: جمع البيانات الشخصية الضرورية فقط لتحقيق الأهداف المعلنة.

ج- الدقة: التأكد من ان البيانات الشخصية دقيقة وحديثة، مع تمكين الافراد من تصحيح البيانات غير الصحيحة.

د- التخزين المحدود: الاحتفاظ بالبيانات الشخصية فقط للمدة التي تكون ضرورية للأغراض التي جمعت من اجلها.

ه- حماية سرية المعلومات: حماية البيانات من الوصول عير المصرح به او الفقدان او التعديل او الإفصاح.

5. حوكمة البيانات الشخصية والامتثال لنظام حماية البيانات

أ- توثيق نموذج الحوكمة: اعتماد خطة لحوكمة البيانات الشخصية وفقاً لنظام حماية البيانات الشخصية ولوائحه. تتضمن الخطة اليات واضحة على شكل سياسات متعددة تغطي جميع الجوانب المطلوبة وتهدف الى تنظيم عملية معالجة البيانات الشخصية بما يتوافق مع القوانين الوطنية.

ب- تحديد الأدوار والمسؤوليات: تشمل ملفات السياسات تحديد الأدوار والمسؤوليات الخاصة بحوكمة البيانات الشخصية، مع توزيع مهام كل جهة او موظف بشكل لا لبس فيه، بحيث يسهم كل دور في تحقيق الامتثال الكامل للنظام.

ج- خطوط التقارير: يجب انشاء خطوط تقارير واضحة ومحددة تتيح المتابعة المستمرة للامتثال لنظام حماية البيانات الشخصية ولوائحه التنفيذية. تسهم هذه الخطوط في دعم الشفافية داخل المؤسسة وتسهيل التقارير حول أي مخالفات او تحديات.

ح- معالجة حالات التعارض: في حال وجود تعارضات داخلية فيما يتعلق بتنفيذ نظام حماية البيانات الشخصية، يجب ان تتبنى الشركة اليات فعالة لتحديد هذه التعارضات ومعالجتها بسرعة وكفاءة، بما يضمن تطبيق السياسات بشكل منسق ومنسجم مع متطلبات النظام

6. الإفصاح عن البيانات الشخصية

أ- يجب ان يكون الإفصاح عن البيانات التي تم جمعها من مصادر متاحة للعموم متوافقة مع النظام ولوائحه.

ب- عند الإفصاح يجب أن:

- يرتبط الإفصاح بغرض محدد وواضح.
- يتم المحافظة على خصوصية صاحب البيانات.
- يقتصر الإفصاح على الحد الأدنى من البيانات اللازمة لتحقيق الغرض.

ج- عند الإفصاح لجهة عامة لأغراض امنية او صحية:

- يتم توثيق الطلب بدقة.
- يحدد نوع البيانات المطلوب الإفصاح عنها.

د- إذا كانت البيانات مرتبطة بشخص أخر غير صاحبها، يتم:

- الموازنة بين حقوق الافراد.
- ترميز هوية الشخص الاخر عند الإمكان.

ه- يجب توثيق جميع عمليات الإفصاح في سجلات خاصة.

7. جمع البيانات الشخصية

أ- مصادر البيانات الشخصية: تجمع جهة التحكم البيانات الشخصية من عدة مصادر تشمل:

- صاحب البيانات مباشرة عند تقديم الخدمات. ويشترط إبلاغه التالي:

- اسم جهة التحكم وبيانات التواصل.
- بيانات مسؤولية حماية البيانات ان وجد.
- المسوغ النظامي والغرض من جمع البيانات.
- مدة الاحتفاظ بالبيانات.
- حقوق صاحب البيانات وآلية ممارستها.
- كيفية العدول عن الموافقة.
- إذا كان جمع البيانات الزامياً او اختيارياً.

- الأطراف الثالثة مثل الشركاء التجاريين.

- المصادر المتاحة للعموم، وذلك للضرورة.

ب- الموافقة:

- ان يتم طلب الموافقة من أصحاب البيانات بطريق صحيحة بدون تضليل.
- ان تكون الموافقة صريحة في حال البيانات المطلوب معالجتها حساسة او ائتمانية، او سيتم اتخاذ قرار بناء على المعالجة الالية للبيانات الشخصية.
- توضيح أغراض الجمع والمعالجة قبل طلب الموافقة.
- توثيق الموافقة بوسيلة تقنية يمكن العودة اليها مستقبلا.
- الحصول على موافقة مستقلة لكل غرض من أغراض الجمع والمعالجة.
- ان تصدر الموافقة من صاحب البيانات كامل الاهلية، او من وليه الشرعي.

- **إذا كان صاحب البيانات الشخصية ناقصاً او فاقداً للأهلية، فيحق لوليه الشرعي:**

- ممارسة حقوق صاحب البيانات وفق النظام واللائحة.
- الموافقة على معالجة بياناته وفق الاحكام.

- **عند معالجة بيانات ناقص او عديم الاهلية:**

- التحقق من صحة الولاية الشرعية.
- ضمان عدم الحاق الضرر بمصالح صاحب البيانات.
- تمكين صاحب البيانات من ممارسة حقوقه عن اكتمال الاهلية.

ت- جمع البيانات الحساسة: تتطلب معالجة البيانات الحساسة موافقة خاصة ويتم جمعها فقط عند الضرورة. مع تطبيق اعلى مستويات الحماية.

د- جمع الحد الأدنى:

- على جهة التحكم جمع الحد الأدنى من البيانات الشخصية الضرورية لتحقيق الغرض من المعالجة.
- يجب ان تكون البيانات مرتبطة مباشرة بالغرض من المعالجة.
- بذل العناية اللازمة لضمان عدم جمع بيانات غير ضرورية.
- تحديد وتدوين الحاجة المباشرة لهذه البيانات والتوقف عن استخدام هذه البيانات في حال انقضاء الضرورة.

ه- جمع البيانات من غير صاحبها مباشرة:

- يجب ان تكون المعالجة ضرورية ومتناسبة مع الغرض المحدد، وان لا تؤثر على حقوق ومصالح صاحب البيانات، وعلى جهة التحكم الاحتفاظ ما يثبت تعذر الاتصال بصاحب هذه البيانات او صعوبة الوصول اليه.
- يجب ابلاغ صاحبها بعملية جمع البيانات خلال مدة لا تزيد عن ثلاثين يوماً.
- عند جمع البيانات من مصدر متاح للعموم، يجب ان يكون ذلك بشكل نظامي.
- في حالة المعالجة، يجب مراعاة إخفاء الهوية حسب المادة التاسعة من اللائحة التنفيذية لنظام حماية البيانات الشخصية.

8. ضوابط معالجة البيانات الشخصية

أ- أغراض المعالجة:

- تتم معالجة البيانات الشخصية من أجل:
- تقديم الخدمات المتفق عليها مع الشركاء.
- أغراض إدارية داخل الشركة مثل التوظيف والتقييم.
- الامتثال للقوانين التنظيمية.

ب- قيود المعالجة:

- يتم استخدام البيانات الشخصية فقط للأغراض المحددة والمعلن عنها، ويتم ابلاغ أصحاب البيانات في حال وجود معالجة إضافية لغرض آخر.
- يحظر استخدام البيانات لأغراض غير مشروعه او تتعارض مع حقوق أصحاب البيانات.

ت- التدابير الأمنية اثناء المعالجة:

- تطبيق تقنيات التشفير عند معالجة البيانات الحساسة.
- تخصيص أدوار وصلاحيات محددو للوصول الى البيانات الشخصية.
- مراقبة أنشطة الوصول لمنع أي تجاوزات او استخدام غير مصرح به.

د- في حال اختيار جهة معالجة، على الجهة التحكم تضمين الاتفاق مع الجهة المعالجة على النحو التالي:

- تتولى جهة التحكم اصدار التعاليم الخاصة للبيانات لجهة المعالجة، وفي حال مخالفتها للتعليمات فعلى الجهة المعالجة اخطار جهة التحكم كتابة وفورياً.
- الغرض من المعالجة.
- المدة الزمنية للمعالجة.
- التزام جهة المعالجة بإشعار جهة التحكم في حال تسريب البيانات الشخصية دون تأخير.
- توضيح ما إذا كانت جهة المعالجة تخضع لأنظمة في دول أخرى، وأثر ذلك على التزامها بأحكام النظام المعمول به داخل المملكة.
- الا يتم اشتراط حصول الجهة المعالجة على موافقة مسبقة بالإفصاح الوجوبي من قبل جهة التحكم، وعلى الأول اشعار الثاني على الإفصاح.
- على جهة التحكم ان تتأكد من التزام الجهة المعالجة بالأنظمة والقوانين الخاصة بالبيانات بشكل دوري، وللأول الاحقية بالاستعانة بطرف خارجي للتأكد من ذلك.
- تعامل جهة المعالجة كجهة التحكم في حال مخالفة أنظمة وقوانين البيانات الخاصة بجهة التحكم.

ه- في حال استعانة الجهة المعالجة بطرف فرعي:

- ضمان عدم تأثر سلامة وامن البيانات المعالجة.
- اخذ الموافقة المسبقة من جهة التحكم على الاستعانة بطرف فرعي.

9. سجل معالجة البيانات الشخصية

- يتم الاحتفاظ بسجلات تفصيلية فيما يتعلق بمعالجة البيانات الشخصية، ويجب الاحتفاظ بهذا السجل لمدة (خمسة سنوات) من بعد انتهاء عملية المعالجة، وعلى الجهة المعالجة توفيرها في حال طلبها من أصحاب البيانات والجهات المختصة، وتشمل السجلات:

أ- هوية المسؤول عن معالجة البيانات.
ب- تفاصيل جهة التحكم.
ج- الجهات التي لها صلاحية الاطلاع على هذه البيانات.
د- وصف فئة هذه البيانات.
ه- الهدف من جمع هذه البيانات.
و- مدة الاحتفاظ بالبيانات.

10. تخزين البيانات الشخصية

أ- المنصة الرقمية والتخزين السحابي:

- تخزن البيانات الشخصية على أنظمة آمنة تضمن حماية البيانات من الهجمات الالكترونية.
- في حال استخدام خدمات التخزين السحابي، يتم التأكد من ان المزود يمتثل لمعايير الأمان وحماية البيانات.

ب- الوصول المصرح به:

- تطبق سياسة صارمة لضمان ان الافراد المخولين فقط هم من يستطيعوا الوصول الى البيانات الشخصية.
- يتم تسجيل وتوثيق كل عملية وصول للبيانات لضمان الشفافية.

ج- قيود زمنية:

- يتم الاحتفاظ بالبيانات الشخصية فقط للفترات الضرورية، وبعد انتهاء الحاجة لها يتم اتلافها بشكل آمن.

11. مشاركة البيانات مع الأطراف الخارجية

أ. اتفاقيات مشاركة البيانات:

- لا تشارك البيانات الشخصية مع أطراف خارجية الا بناءً على اتفاقيات رسمية تضمن الموافقات المسبقة وسرية المعلومات والامتثال للقوانين.
- تضمن الاتفاقيات بنوداً حول حماية البيانات والامتثال للمتطلبات القانونية.

ب. إجراءات امان الطرف الثالث:

- يتم إجراءات الأمان لدى الأطراف الخارجية قبل توقيع الاتفاقيات.
- يتم متابعة الامتثال بشكل دوري من خلال تدقيقات دورية.

12. حماية البيانات الائتمانية

أ. **اتخاذ الإجراءات للحماية:** يجب على جهة التحكم تنفيذ إجراءات تنظيمية وتقنية وفنية لضمان حماية البيانات الائتمانية من أي استخدام غير مشروع، والتأكد من عدم الاطلاع عليها من قبل غير المصرح لهم، واستخدامها فقط للأغراض التي جمعت من اجلها، ومنع تسريبها.

ب. **الامتثال لمتطلبات البنك المركزي:** يجب على جهة التحكم تبني وتطبيق الاشتراطات والضوابط التي يصدرها البنك المركزي السعودي والجهات الأخرى ذا العلاقة.

ت. **موافقة صاحب البيانات:** يجب على جهة التحكم الحصول على موافقة صاحب البيانات الشخصية وابلاغه عند وجود أي طلب للإفصاح عن بياناته الائتمانية.

13. حماية البيانات الصحية

في احتاجت جهة التحكم للتعامل مع البيانات الصحية فيلزم ما يلي:

أ. **اتخاذ الإجراءات للحماية:** اتخاذ إجراءات تنظيمية وتقنية وفنية لحماية البيانات الصحية من الاستعمال غير المشروع، او استخدامها لغير الغرض الذي جمعت من اجله، او تسريبها، وضمان خصوصية أصحاب البيانات.

ب. **تبني وتطبيق الاشتراطات والضوابط:** الصادرة عن وزارة الصحة، المجلس الصحي السعودي، البنك المركزي السعودي، مجلس الضمان الصحي، والجهات الأخرى ذا العلاقة.

ج. تضمين الاحكام الواردة في النظام ولوائحه في السياسات الداخلية لدى جهة التحكم، وتوزيع المهام والمسؤوليات بوضوح لتجنب تداخل الاختصاصات.

د. توثيق جميع مراحل معالجة البيانات الصحية وتحديد المسؤولين عن كل مرحلة.

14. إخفاء الهوية

حسب اللائحة التنفيذية لنظام حماية البيانات الشخصية، البيانات التي تم إخفاء هوية صاحبها لا تعد بيانات شخصية، ويجب على جهة التحكم عند إخفاء هوية صاحب البيانات الشخصية التأكد من التالي:

أ. عدم إمكانية إعادة التعرف على هويته.

ب. تقويم الأثر لضمان عدم إمكانية إعادة تحديد الهوية.

ج. اتخاذ التدابير اللازمة لتجنب المخاطر، مع تحديث التقنيات وفق التطورات.

د. تقويم أثر فاعلية تقنيات إخفاء الهوية وتعديلها عند الضرورة.

15. حقوق أصحاب البيانات

أ- الوصول الى البيانات الشخصية: يحق لصاحب البيانات:
- طلب الوصول الى البيانات الشخصية التي تحتفظ بها الشركة.
- طلب معلومات حول كيفية معالجة البيانات.

ب- تصحيح وحذف البيانات: لصاحب البيانات الحق في طلب تصحيح البيانات الشخصية غير الصحيحة او حذفها إذا لم تعد هناك حاجة لها.

ج- حق الاعتراض: يحث للأفراد على معالجة بياناتهم الشخصية لأغراض محددة، مثل التسويق المباشر.

د- يجب على جهة التحكم توفير وسائل ملائمة لتمكين صاحب البيانات الشخصية من ممارسة حقوقه، ومنها: البريد الالكتروني، الرسائل النصية، العنوان الوطني، التطبيقات الالكترونية، أو أي وسيلة نظامية أخرى.

16. التدابير الأمنية لحماية البيانات

أ. الحلول التكنولوجية

- يتم استخدام تقنيات التشفير والجدران النارية لحماية البيانات من الاختراق.
- يتم استخدام حلول النسخ الاحتياطي وذلك لحفظ الملفات من أي حادث قد يتسبب في فقدان البيانات.
- يتم عمل اختبارات استعادة وذلك لضمان نجاح واستمرارية عمليات النسخ الاحتياطي.
- يستخدم التحكم في الوصول لضمان ان الموظفين المصرح لهم فقط يمكنهم الوصول الى البيانات الحساسة.

ب. التدابير التنظيمية.

- يتم تدريب الموظفين على حماية البيانات والتوعية بالمخاطر المرتبطة بها.
- تنفذ مراجعات دورية لضمان الامتثال للسياسات والمعايير.

17. الامتثال

أ- خطط الاستجابة للحوادث: يتم وضع خطط استجابة شاملة لحالات خرق البيانات تتضمن اشعار السلطة والافراد المعنيين.

ب- مراجعة الامتثال

- تجري الشركة عمليات تدقيق دورية لضمان الامتثال لجميع السياسات واللوائح المتعلقة بحماية البيانات الشخصية.
- يتم اعداد تقارير دورية لمراجعة الامتثال ورفعها للإدارة العليا.

ج- إجراءات التصحيح: في حال اكتشاف أي تجاوزات او انتهاكات للسياسات، يتم اتخاذ إجراءات تصحيحه فورية، مع مراجعة جميع الأنظمة المعنية لضمان عدم تكرار الحوادث.

18. العدول عن الموافقة

لأصحاب البيانات الشخصية حق العدول عن موافقته في معالجة بياناته في أي وقت، مع ابلاغ جهة التحكم بذلك. ويجب على جهة التحكم:

أ. توفير اجراءات سهلة للعدول عن الموافقة، وتكون أسهل من إجراءات الحصول على الموافقة.
ب. إيقاف الموافقة فوراً بعد العدول.
ج. اشعار من تم الإفصاح لهم عن البيانات وطلب اتلافها.

- **العدول لا يؤثر على مشروعية المعالجة السابقة ولا على المعالجة بناءً على مسوغات نظامية أخرى.**

19. تقويم الأثر

أ. يجب على جهة التحكم اعداد تقويماً مكتوباً وموثقاً لتقييم الاثار والمخاطر التي قد تلحق بصاحب البيانات الشخصية نتيجة معالجة بياناته.

ب. يتم اجراء تقويم الأثر في الحالات التالية:
- عند معالجة البيانات الشخصية الحساسة.
- عند جمع او ربط مجموعتين او أكثر من البيانات من مصادر مختلفة.
- عند معالجة بيانات لناقصي، او عديمي الاهلية، او استخدام تقنيات ناشئة، او اتخاذ قرارات مبنية على المعالجات الآلية.

ج- يجب ان يتضمن تقويم الأثر على العناصر التالية:
- الغرض من المعالجة والاساس القانوني لها.
- وصف لأنواع البيانات ونطاق المعالجة.
- العلاقة بين أصحاب البيانات ونطاق المعالجة.

د- تقييم الاثار السلبية المحتملة، سواء كانت اجتماعية، مالية، او غيرها.
ه- اتخاذ التدابير المناسبة لمنع المخاطر او الحد منها.
و- في حال اظهر التقويم ان المعالجة ستؤدي الى الاضرار بخصوصية الافراد، يجب معالجة هذه الأسباب وإعادة التقويم.

20. إدارة الحوادث والتسريب

أ. خطة الاستجابة للحوادث:
- في حال وقوع أي حادث يتعلق بتسريب البيانات الشخصية او وصول غير مصرح به، يجب تنفيذ خطة الاستجابة للحوادث.
- الاشعار الفوري للبنك المركزي خلال (72) ساعة من اكتشاف الحادث.

ب- يتضمن الاشعار:
- وصف لحادثة تسرب البيانات، مع تحديد وقت وتاريخ وكيفية وقوعها ووقت علم جهة التحكم بها.
- الفئات والاعداد الفعلية او التقريبية لأصحاب البيانات الشخصية المتأثرين، ونوع البيانات التي تم تسريبها
- وصف للمخاطر المحتملة الناتجة عن الحادثة، مع توضيح الإجراءات المتخذة لتخفيف الاثار والتدابير المستقبلية لمنع تكرار الحادثة.

ج- بيان حول ما إذا تم او سيتم اشعار صاحب البيانات المتأثر بالتسريب.
د- إذا لم تتمكن جهة التحكم من تقديم المعلومات المطلوبة خلال (72) ساعة، فعليها تقديمها في أقرب وقت ممكن مع تقديم مبررات التأخير.
ه- تحتفظ جهة التحكم بنسخة من التقارير المقدمة للجهة المختصة، وتوثق التدابير التصحيحية المتخذة، واي مستندات ذات صلة.
و- لا تخل احكام هذه السياسة بأي التزامات أخرى لجهة التحكم او المعالجة بتقديم تقارير لحوادث التسريب وفقاً لما تحدده الهيئة الوطنية للأمن السيبراني او الأنظمة الأخرى المعمول بها.
ز- على جهة التحكم اشعار صاحب البيانات الشخصية دون تأخير غير مبرر اذا كان من شأن الحادثة ان تسبب ضرراً لبياناته او تتعارض مع حقوقه.

ح- يجب ان يتضمن الاشعار لصاحب البيانات:

- وصف الحادثة.
- وصف المخاطر المحتملة والتدابير المتخذة للحد منها.
- اسم وبيانات التواصل لجهة التحكم او مسؤول حماية البيانات الشخصية.
- توصيات او نصائح لتجنب المخاطر وتخفيف اثارها.

ط- يجب ان يكون الاشعار بلغة مبسطة وواضحة لصاحب البيانات.

ي- تلتزم جهة التحكم بالتعاون مع الجهات المختصة لضمان معالجة الحادثة واتخاذ الإجراءات اللازمة لمنع تكرارها.

21. التدريب والنوعية

أ- **برامج التدريب:** يتم تنظيم برامج تدريبية مستمرة للموظفين لرفع وعيهم حول السياسات الخاصة بحماية البيانات وكيفية التعامل معها بشكل آمن.

ب- **حملات التوعية:** يتم تنفيذ حملات توعية داخلية لزيادة فهم الموظفين لكيفية حماية البيانات الشخصية والامتثال للسياسات.

ج- **تقييم الأداء:** يتم تقييم أداء الموظفين في التعامل مع البيانات الشخصية ضمن إطار مؤشرات الأداء لضمان تحسين مستمر.

22. التخلص من البيانات (الاتلاف)

أ- سياسة الاتلاف:

- عندما لا تعود البيانات الشخصية ضرورية للأغراض التي تم جمعها من اجلها او تم انتهاء علاقة العمل مع الشركاء، يجب اتلافها بشكل آمن.
- بناءً على طلب صاحب البيانات.
- إذا عدل صاحب البيانات عن موافقته، وكانت الموافقة هي السبب الوحيد للمعالجة.
- إذا تم اكتشاف معالجة البيانات بشكل مخالف للنظام.
- يتم استخدام إجراءات مثل الحذف النهائي من الأنظمة او تدمير الوسائط التي تحتوي على البيانات.

ب- التوثيق:

- يتم توثيق جميع عمليات اتلاف البيانات لضمان الامتثال للسياسات.

ج- تكوين لجنة اتلاف:

- من داخل الشركة تضمن تنفيذ السياسة المذكورة وتصدر خطاباً يفيد بتنفيذ الاتلاف بشكل كلي.

د- عند الاتلاف يجب اشعار الجهات الأخرى التي تم الإفصاح لها وطلب اتلاف البيانات، بالإضافة الى اتلاف جميع النسخ بما في ذلك النسخ الاحتياطية، مع مراعاة المتطلبات النظامية.

23. التحديثات والتعديلات على السياسة

أ- **المراجعة الدورية:** تراجع هذه السياسة بانتظام لضمان توافقها مع القوانين والتطورات الجديدة في مجال حماية البيانات.

ب- **التعديلات الطارئة:** يتم تعديل السياسة فوراً إذا دعت الحاجة لذلك نتيجة لتغييرات قانونية او تنظيمية تؤثر على حماية البيانات الشخصية.

24. أمن المعلومات

يجب على جهة التحكم اتخاذ التدابير للازمة لضمان أمن البيانات الشخصية وخصوصية أصحابها، بما يشمل:

أ- تطبيق التدابير الأمنية والتقنية للحد من مخاطر تسرب البيانات.

ب- الالتزام بضوابط ومعايير الامن السيبراني الصادرة عن الهيئة الوطنية للأمن السيبراني، او اتباع أفضل ممارسات الامن السيبراني المعترف بها في حال عدم إلزام جهة التحكم بتطبيق ضوابط الهيئة.