

سياسة مؤسسية

سياسة حماية البيانات الشخصية

قواعد حماية البيانات الشخصية وحقوق أصحابها ومسؤوليات معالجتها في الجامعة

الإصدار	تاريخ الإصدار	المراجعة القادمة	التصنيف
1.0	2025-12-31	2027-12-31	عام

المملكة العربية السعودية، حفر الباطن · ص.ب 1803 · الرمز البريدي 31991
هاتف 013 7203426 · فاكس 013 7247212 · www.uhb.edu.sa

رؤية 2030 VISION
المملكة العربية السعودية
KINGDOM OF SAUDI ARABIA

ضبط الوثيقة

تفاصيل الوثيقة

اسم الوثيقة	سياسة حماية البيانات الشخصية
المؤسسة	جامعة حفر الباطن
مالك الوثيقة	مكتب إدارة البيانات
رقم الإصدار	1.0
الحالة	إصدار
تاريخ الإصدار	2025-12-31
تاريخ المراجعة القادمة	2027-12-31
تصنيف الوثيقة	عام

جدول اعتماد الوثيقة

الإصدار	التاريخ	التعديلات	تحرير	مراجعة	موافقة
1.0	2025-12-31	لا يوجد	**أ. شهد منصور الشمري**	**أ. صالح عامر العنزي** مسؤول إتاحة البيانات	**أ.د. محمد متعب العتيبي** المشرف على مكتب إدارة البيانات

الموافقات

الاسم / الجهة	الوظيفة / رقم المحضر	التاريخ
أ.د. محمد متعب العتيبي	المشرف على مكتب إدارة البيانات	2025-12-31
لجنة التعاملات الإلكترونية (اللجنة التوجيهية)	رقم المحضر: 2253-1-2002-5	1447-07-21
رقم قرار الاعتماد من لجنة المعاملات الإلكترونية	رقم المحضر: 2252-1-1232-1	1447-10-24

سجل الإصدارات

رقم الإصدار	تاريخ المراجعة	المساهم	التعديل
1	2025-12-31	مكتب إدارة البيانات	الإصدار الأول

المحتوى

جدول التعريفات 4

أولًا المقدمة 6

ثانيًا المبادئ الرئيسية لحماية البيانات الشخصية 7

ثالثًا القواعد العامة لحماية البيانات الشخصية 8

رابعًا بيان السياسة 9

خامسًا الأدوار والمسؤوليات 24

بيانات التواصل 26

الوثائق ذات العلاقة 26

المراجع 26

جدول التعريفات

المصطلح	التعريف
الجامعة	جامعة حفر الباطن
إدارات الجامعة	الوكالات، العمادات، الوحدات، الإدارات، الأقسام.
البيانات	مجموعة من الحقائق في صورتها الأولية أو في صورة غير منظمة، مثل: الأرقام، أو الحروف، أو الصور الثابتة، أو الفيديو، أو التسجيلات الصوتية، أو الرموز التعبيرية.
البيانات الشخصية	كل بيان - مهما كان مصدره أو شكله - من شأنه أن يؤدي إلى معرفة الفرد على وجه التحديد، أو يجعله قابلاً للتعرف عليه بصفة مباشرة أو غير مباشرة عند دمجه مع بيانات أخرى، ويشمل ذلك - على سبيل المثال لا الحصر - الاسم، وأرقام الهويات الشخصية، والعناوين، وأرقام التواصل، وأرقام الحسابات البنكية والبطاقات الائتمانية، والبيانات الصحية، وصور المستخدم الثابتة أو المتحركة، وغير ذلك من البيانات ذات الطابع الشخصي أو ذات السمة الخاصة التي يستدل منها على فرد معين.
الوصول للبيانات	القدرة على الوصول المنطقي والمادي إلى البيانات والموارد التقنية للجامعة، لغرض استخدامها.
صاحب البيانات الشخصية	الشخص الطبيعي الذي تتعلق به البيانات الشخصية أو من يمثله أو من له الولاية الشرعية عليه.
معالجة البيانات الشخصية	جميع العمليات التي تُجرى على البيانات الشخصية بأي وسيلة كانت يدوية أو آلية، وتشمل هذه العمليات - على سبيل المثال لا الحصر - جمع البيانات ونقلها وحفظها وتخزينها ومشاركتها وإتلافها وتحليلها واستخراج أنماطها والاستنتاج منها وربطها مع بيانات أخرى.
الافصاح عن البيانات الشخصية	تمكين أي شخص – ماعدا مكتب إدارة البيانات في الجامعة - من الحصول على البيانات الشخصية أو استعمالها أو الاطلاع عليها أو الوصول إليها بأي وسيلة ولأي غرض.
تسريب البيانات الشخصية	الإفصاح عن البيانات الشخصية، أو الحصول عليها، أو تمكين الوصول إليها دون تصريح أو سند نظامي، سواءً بقصد أو بغير قصد.

المصطلح	التعريف
اتلاف البيانات الشخصية	أي عمل يؤدي إلى إزالة البيانات الشخصية ويجعل من المتعذر الاطلاع عليها أو استعادتها مرة أخرى، بما في ذلك المسح والحذف سواءً كان ذلك إلكترونياً أو مادياً.
إشعار الخصوصية	هو بيان خارجي موجه للأفراد يوضح محتوى البيانات الشخصية ووسائل جمعها والغرض من معالجتها وكيفية استخدامها والجهات ذات العلاقة التي سيتم مشاركة هذه البيانات معها وفترة الاحتفاظ بها وآلية التخلص منها.
مستويات تصنيف البيانات	مستويات تصنيف البيانات هي: سري للغاية، سري، مقيد، عام.
التسويق المباشر	التواصل مع صاحب البيانات الشخصية بأي وسيلة مادية أو إلكترونية مباشرة بهدف توجيه مادة تسويقية، ويشمل ذلك على سبيل المثال لا الحصر الإعلانات أو العروض الترويجية.
المصلحة الحيوية	أي من المصالح الضرورية للحفاظ على حياة صاحب البيانات الشخصية.
المصلحة المتحققة	أي مصلحة معنوية أو مادية لصاحب البيانات الشخصية ترتبط بشكل مباشر بالغرض من معالجة البيانات الشخصية، وتكون المعالجة ضرورية لتحقيق تلك المصلحة.
المصلحة المشروعة	أي حاجة ضرورية لدى جهة التحكم يتطلب تحقيقها معالجة بيانات شخصية لغرض محدد، على ألا تؤثر على حقوق ومصالح صاحب البيانات الشخصية.
الترميز	تحويل المعرفات الرئيسية التي تدل على هوية صاحب البيانات الشخصية إلى رموز تحول دون التعرف المباشر على هوية صاحب البيانات الشخصية دون استخدام بيانات أو معلومات إضافية، وأن يتم الاحتفاظ بالبيانات أو المعلومات الإضافية بشكل منفصل، ووضع الضوابط الفنية والإدارية اللازمة لضمان عدم ربطها بهوية صاحب البيانات الشخصية بشكل محدد.
إخفاء الهوية	إزالة المعرفات المباشرة وغير المباشرة التي تدل على هوية صاحب البيانات الشخصية بشكل نهائي يتعذر معه تحديد هوية صاحب البيانات الشخصية.
الموافقة الصريحة	موافقة تمنح بشكل مباشر وصريح من صاحب البيانات الشخصية بأي شكل من الأشكال وتدل على قبوله بمعالجة بياناته الشخصية بحيث لا يمكن تفسيرها بخلاف ذلك، وتكون قابلة للإثبات.

أولًا

المقدمة

1.1 الغرض من الوثيقة

استجابة لضوابط مكتب إدارة البيانات الوطنية والمعايير ذات الصلة بضرورة وضع سياسات حوكمة البيانات في الجهات الحكومية انطلاقاً من سياسات حوكمة البيانات الوطنية التي تم تطويرها انسجاماً مع الجهات الحكومية قام مكتب البيانات في الجامعة بتطوير وثيقة سياسة حماية البيانات الشخصية، بالتوافق مع سياسات مكتب إدارة البيانات الوطنية.

تهدف هذه السياسة إلى وضع القواعد الأساسية لحماية البيانات الشخصية التي يتم معالجتها والتي يجب اتباعها من قبل إدارات الأعمال داخل الجامعة لضمان سلامة البيانات الشخصية لدى المستخدمين.

1.2 نطاق عمل السياسة وتطبيقها

تطبق هذه السياسة على جميع جهات الجامعة التي تتعامل بشكل مباشر أو غير مباشر مع البيانات الشخصية لكافة منسوبي ومنسوبات الجامعة (عضو / عضوة، موظف / موظفة، طالب / طالبة)، وغيرهم ممن يرتبط بعلاقة تعاقدية أو نظامية مع الجامعة.

لا تنطبق أحكام هذه السياسة في الحالات التالية:

- تحقيق متطلبات نظامية وفق الأنظمة واللوائح والسياسات المعمول بها.
- استيفاء متطلبات قضائية.
- تنفيذ التزام بموجب اتفاق تكون المملكة طرفاً فيه.
- حماية الصحة، أو السلامة العامة، أو حماية المصالح الحيوية للأفراد.

1.3 جدول مراجعة السياسة

يجب مراجعة هذه السياسة بشكل منتظم بحيث تكون هذه المراجعة مرة واحدة سنوياً على أقل تقدير وفقاً لما يوجه به المشرف العام على السياسة ويطلب من مكتب إدارة البيانات داخل الجامعة ذلك.

1.4 مراقبة الامتثال

يقاس الامتثال لسياسة حماية البيانات الشخصية وفقاً لمعايير ومؤشرات أداء يضعها مكتب إدارة البيانات في الجامعة وبالتوافق مع متطلبات مكتب إدارة البيانات الوطنية، ويتم مراجعة معايير الامتثال بشكل دوري من قبل مدير مكتب إدارة البيانات.

ثانيًا

المبادئ الرئيسية لحماية البيانات الشخصية

1 المبدأ الأول: المشروعية والعدالة والشفافية

يجب أن تتم معالجة البيانات الشخصية بطريقة مشروعة وعادلة وواضحة لصاحب البيانات، وبما يضمن علمه بكيفية استخدام بياناته وأغراض معالجتها.

2 المبدأ الثاني: تحديد الغرض

تُجمع البيانات الشخصية لأغراض محددة وواضحة ومشروعة، ولا يجوز معالجتها لاحقاً بطريقة تتعارض مع تلك الأغراض.

3 المبدأ الثالث: تقليل البيانات

يقتصر جمع ومعالجة البيانات الشخصية على الحد الأدنى اللازم لتحقيق الغرض المحدد دون زيادة غير مبررة.

4 المبدأ الرابع: دقة البيانات

يجب أن تكون البيانات الشخصية دقيقة ومحدثة، مع اتخاذ الإجراءات اللازمة لتصحيح أو إتلاف البيانات غير الدقيقة.

5 المبدأ الخامس: إتاحة البيانات

تتم إتاحة جميع المعلومات الضرورية المتعلقة بطلب مشاركة البيانات لجميع أطراف عملية مشاركة البيانات، وذلك من خلال إيضاح البيانات المطلوبة ومستويات تصنيفها - بحسب ما تنص عليه سياسة تصنيف البيانات - والغرض من طلبها، وطرق حفظها، والضوابط المستخدمة لحمايتها وآلية إتلافها.

6 المبدأ السادس: تحديد مدة الاحتفاظ

لا يجوز الاحتفاظ بالبيانات الشخصية لمدة أطول من اللازم لتحقيق الغرض الذي جُمعت من أجله، ويجب إتلافها أو إخفاء هويتها بعد انتهاء الغرض.

7 المبدأ السابع: أمن البيانات وسريتها

يجب تطبيق التدابير التنظيمية والفنية المناسبة لحماية البيانات الشخصية من الوصول غير المصرح به أو الإفصاح أو التعديل أو التلف.

8 المبدأ الثامن: المساءلة

تتحمل جهة التحكم المسؤولية الكاملة عن الالتزام بمبادئ ومتطلبات حماية البيانات الشخصية، ويجب أن تكون قادرة على إثبات الامتثال عند الطلب.

ثالثًا

القواعد العامة لحماية البيانات الشخصية

1. تلتزم جامعة حفر الباطن عند تلقيها طلباً من صاحب البيانات الشخصية يتعلق بممارسة أي من الحقوق المنصوص عليها في نظام حماية البيانات الشخصية بما يلي:
   - أ- تنفيذ طلبات ممارسة الحقوق خلال مدة لا تتجاوز (ثلاثين) يوماً من تاريخ استلام الطلب دون تأخير، ويجوز للجامعة تمديد هذه المدة عند الحاجة إذا تطلب تنفيذ الطلب جهداً إضافياً غير متوقع أو غير معتاد، أو في حال تلقي عدة طلبات من صاحب البيانات الشخصية، على ألا تتجاوز مدة التمديد (ثلاثين) يوماً إضافية، شريطة إشعار صاحب البيانات الشخصية مسبقاً بالتمديد وأسبابه.
   - ب- تبني وتطبيق الوسائل التقنية والإدارية والتنظيمية اللازمة لضمان سرعة وكفاءة الاستجابة لطلبات ممارسة حقوق أصحاب البيانات الشخصية.
   - ج- اتخاذ الإجراءات والتدابير المناسبة للتحقق من هوية مقدم الطلب قبل تنفيذ الطلب، بما يتوافق مع الأحكام النظامية ذات العلاقة.
   - د- اتخاذ الوسائل اللازمة لتوثيق وحفظ جميع الطلبات المقدمة إلى الجامعة، بما في ذلك الطلبات المقدمة شفهياً، وفق الضوابط المعتمدة.
2. في حال كان الطلب متكرراً بشكل غير مبرر أو كان تنفيذه يتطلب جهداً غير عادي، يكون لجامعة حفر الباطن عدم معالجة الطلب، على أن يكون ذلك مسبباً، مع إشعار صاحب البيانات الشخصية بذلك.
3. في الحالات التي يكون فيها صاحب البيانات الشخصية ناقص الأهلية أو عديم الأهلية، يحق لوليّه الشرعي ممارسة الحقوق المنصوص عليها في النظام نيابةً عنه.

رابعًا

بيان السياسة

حقوق صاحب البيانات

الحق في العلم

1. الشفافية والإشعار

تلتزم جامعة حفر الباطن بإشعار صاحب البيانات الشخصية قبل جمع بياناته مباشرة أو في أقرب وقت ممكن، متضمناً:

- هوية الجهة المسؤولة عن المعالجة ووسائل التواصل معها.
- الغرض من جمع البيانات، ومعالجتها بشكل واضح ومحدد.
- مدة الاحتفاظ بالبيانات أو معايير تحديدها.

2. حقوق صاحب البيانات الشخصية

توضح الجامعة لأصحاب البيانات حقوقهم النظامية المتعلقة ببياناتهم الشخصية، وآلية ممارسة تلك الحقوق، بما في ذلك حق الاطلاع أو التصحيح أو سحب الموافقة، وفق الأنظمة المعتمدة.

3. الاستثناءات النظامية للإشعار

يجوز للجامعة عدم الإشعار المسبق في الحالات التي ينص عليها النظام، مثل:

- إذا كانت البيانات متاحة مسبقاً لصاحبها.
- إذا كان الإشعار يشكل عبئاً غير معقول.
- إذا كانت المعالجة مطلوبة لتحقيق مصلحة عامة أو لأغراض أمنية أو نظامية.
- إذا كانت البيانات تخضع لأحكام السرية المهنية.

4. المعالجة الآلية والنطاق الواسع

في حال تنفيذ معالجات آلية أو معالجات واسعة النطاق أو متكررة للبيانات الشخصية، تلتزم الجامعة باتخاذ التدابير اللازمة لإشعار أصحاب البيانات، وبيان:

- طبيعة ونطاق المعالجة.
- ما إذا كانت هناك قرارات آلية مؤثرة تُتخذ بناءً على هذه المعالجة.
- الضوابط والإجراءات المعتمدة لحماية البيانات الشخصية.

5. المعالجة الإضافية للبيانات

عند الرغبة في إجراء معالجة إضافية غير الغرض الأصلي الذي جُمعت من أجله البيانات، تلتزم الجامعة بإشعار صاحب البيانات مسبقاً وتقديم المعلومات اللازمة وفقاً للأحكام النظامية.

6. وضوح المعلومات وسهولة الوصول

تحرص الجامعة على أن تكون جميع المعلومات المقدمة لأصحاب البيانات واضحة، ومفهومة، ومكتوبة بلغة مناسبة، وبما يضمن تمكينهم من ممارسة حقوقهم بيسر وفاعلية.

الحق في الوصول إلى البيانات الشخصية

1. حق الاطلاع والوصول

تُمكّن جامعة حفر الباطن صاحب البيانات الشخصية من الوصول إلى بياناته الشخصية المحتفظ بها لديها، وذلك وفقاً للأحكام النظامية المعتمدة، ودون الإخلال بالاستثناءات المنصوص عليها نظاماً.

2. نطاق ممارسة الحق

يشمل حق الوصول تمكين صاحب البيانات من الاطلاع على بياناته الشخصية، بما لا يؤدي إلى الإضرار بحقوق الآخرين، أو كشف بيانات شخصية لطرف آخر، أو الإخلال بالأنظمة ذات العلاقة.

3. آلية تقديم الطلب

يتم تمكين صاحب البيانات من ممارسة حقه في الوصول من خلال طلب رسمي يقدمه عبر القنوات المعتمدة لدى الجامعة، وتلتزم الجامعة بتوفير وسيلة واضحة وميسّرة لاستقبال هذه الطلبات. وذلك من خلال بريد مكتب إدارة البيانات الرسمي dmo@uhb.edu.sa

4. التحقق والحماية

تلتزم الجامعة بالتحقق من هوية مقدم الطلب قبل تمكينه من الوصول إلى بياناته، بما يضمن حماية البيانات الشخصية ومنع الإفصاح غير المصرح به.

الحق في طلب الوصول إلى البيانات الشخصية

1. حق طلب نسخة من البيانات

يحق لصاحب البيانات الشخصية طلب الحصول على نسخة من بياناته الشخصية المحتفظ بها لدى جامعة حفر الباطن، وذلك وفقاً للأحكام النظامية المعتمدة، وبما لا يمس حقوق الغير أو الحقوق المحمية نظاماً.

2. وسيلة تقديم البيانات

تلتزم الجامعة بتوفير البيانات الشخصية المطلوبة بصيغة إلكترونية واضحة وسهلة الاستخدام متى ما كان ذلك ممكناً، وبما يحقق الغرض من الطلب.

3. حماية حقوق الآخرين

عند تنفيذ طلب الحصول على البيانات، تلتزم الجامعة باتخاذ الإجراءات اللازمة لضمان عدم الإفصاح عن أي بيانات شخصية تتعلق بأطراف أخرى.

الحق في طلب تصحيح البيانات الشخصية

1. طلب التصحيح أو التحديث

يحق لصاحب البيانات الشخصية طلب تصحيح أو تحديث بياناته الشخصية لدى جامعة حفر الباطن في حال كانت غير دقيقة أو غير مكتملة، وذلك وفقاً للإجراءات النظامية المعتمدة.

2. آلية التحقق والتنفيذ

للجامعة طلب ما يلزم من مستندات أو بيانات داعمة للتحقق من صحة طلب التصحيح، ويتم تحديث البيانات أو إيضاح أسباب عدم التنفيذ خلال المدة النظامية المحددة.

3. إشعار الجهات ذات العلاقة

تلتزم الجامعة، متى ما كان ذلك ممكناً، بإشعار الجهات التي سبق الإفصاح لها عن البيانات الشخصية بأي تصحيح أو تحديث يطرأ عليها، دون تأخير غير مبرر.

الحق في طلب إتلاف البيانات الشخصية

1. طلب الإتلاف

تلتزم جامعة حفر الباطن بإتلاف البيانات الشخصية بناءً على طلب صاحبها في أي من الحالات التالية:

- انتهاء الغرض الذي جُمعت من أجله البيانات.
- سحب موافقة صاحب البيانات على معالجتها، متى ما كانت المعالجة قائمة على الموافقة.
- ثبوت جمع أو معالجة البيانات بطريقة مخالفة للأنظمة المعتمدة.

2. إجراءات الإتلاف

عند إتلاف البيانات الشخصية، تلتزم الجامعة باتخاذ الإجراءات اللازمة لضمان:

- إشعار الجهات التي سبق الإفصاح لها عن البيانات، متى ما كان ذلك ممكناً.
- إشعار صاحب البيانات بإتمام عملية الإتلاف عند الطلب.

3. الاستثناءات النظامية

لا يخل تنفيذ إتلاف البيانات بالالتزامات النظامية التي تُلزم الجامعة بالاحتفاظ ببعض البيانات وفق أنظمة أخرى أو متطلبات نظامية ذات علاقة.

إخفاء الهوية

1. متطلبات إخفاء الهوية

عند إخفاء هوية البيانات الشخصية، تلتزم جامعة حفر الباطن بما يلي:

- ضمان عدم إمكانية إعادة التعرف على صاحب البيانات بعد إخفاء هويته.
- تطبيق أساليب وتقنيات مناسبة لإخفاء الهوية بما يتوافق مع أفضل الممارسات الفنية والتنظيمية.

2. إدارة المخاطر والمراجعة

تقوم الجامعة بتقييم مخاطر إعادة التعرف بشكل دوري، ومراجعة تقنيات إخفاء الهوية وتحديثها كلما دعت الحاجة، بما يضمن استمرار فاعلية الإخفاء.

3. نطاق التطبيق

لا تُعد البيانات التي أُخفيت هويتها بيانات شخصية، ولا تخضع لأحكام حماية البيانات الشخصية متى ما استوفت متطلبات إخفاء الهوية النظامية.

وسائل التواصل

تلتزم جامعة حفر الباطن بتوفير وسائل تواصل واضحة ومناسبة لتمكين أصحاب البيانات الشخصية من تقديم طلباتهم وممارسة حقوقهم النظامية، وتشمل – بحسب ما تتيحه الأنظمة – القنوات التالية:

- البريد الإلكتروني الرسمي dmo@uhb.edu.sa.
- الرسائل النصية.
- العنوان الوطني.
- البوابات أو التطبيقات الإلكترونية المعتمدة.
- أي قنوات رسمية أخرى تحددها الجامعة.

الموافقة على معالجة البيانات الشخصية

1. أساس الموافقة

تحصل الجامعة على موافقة صاحب البيانات الشخصية قبل معالجتها متى ما كان ذلك مطلوباً نظاماً، سواء كانت الموافقة كتابية أو إلكترونية أو بأي وسيلة معتمدة.

2. ضوابط الموافقة

يجب أن تكون الموافقة:

- صريحة ومحددة الغرض.

- واضحة وغير مشروطة بالخدمات الأساسية ما لم ينص النظام على خلاف ذلك.
- قابلة للإثبات والتوثيق.

3. إدارة الموافقات

تلتزم الجامعة بتوثيق الموافقات والاحتفاظ بها، وتمكين صاحب البيانات من سحب موافقته في أي وقت، ما لم توجد متطلبات نظامية أخرى تقتضي الاستمرار في المعالجة.

4. الحالات الخاصة

يشترط الحصول على موافقة صريحة في الحالات التالية:

- معالجة البيانات الحساسة.
- معالجة بيانات الأطفال.
- اتخاذ قرارات آلية مؤثرة اعتماداً على البيانات الشخصية.

العدول عن الموافقة

1. حق العدول

يحق لصاحب البيانات الشخصية العدول عن موافقته على معالجة بياناته في أي وقت، وذلك وفق الإجراءات المعتمدة لدى جامعة حفر الباطن.

2. أثر العدول

يترتب على العدول إيقاف معالجة البيانات المرتبطة بالموافقة، دون أن يؤثر ذلك على المعالجات التي تمت قبل العدول بصورة نظامية.

3. إشعار الجهات ذات العلاقة

تلتزم الجامعة، متى ما كان ذلك ممكناً، بإشعار الجهات التي تم الإفصاح لها عن البيانات الشخصية بواقعة العدول وطلب إيقاف المعالجة.

4. الاستثناءات النظامية

لا يؤثر العدول عن الموافقة على المعالجات القائمة على مسوغات نظامية أخرى غير الموافقة.

موافقة الولي الشرعي

1. الحالات التي تتطلب موافقة الولي

تشترط جامعة حفر الباطن الحصول على موافقة الولي الشرعي عند معالجة بيانات شخصية تعود لقاصر أو شخص عديم الأهلية، وذلك وفقاً للأحكام النظامية.

2. ضوابط الموافقة

يجب التحقق من صفة الولي الشرعي وأهليته نظاماً قبل اعتماد الموافقة، مع توثيقها بالوسائل المعتمدة.

3. حماية حقوق صاحب البيانات

لا يترتب على موافقة الولي الشرعي أي إخلال بحقوق صاحب البيانات الشخصية، وتظل هذه الحقوق محفوظة وقابلة للممارسة عند اكتمال الأهلية.

جمع البيانات من غير صاحبها مباشرة

1. يجوز للجامعة جمع البيانات الشخصية من مصادر أخرى غير صاحبها مباشرة متى ما كانت المعالجة ضرورية ومتناسبة مع الغرض المحدد، ودون المساس بحقوق صاحب البيانات.
2. تلتزم الجامعة بأن تكون مصادر البيانات نظامية ومشروعة، وبما لا يخالف الأنظمة ذات العلاقة.
3. تطبق الجامعة أحكام الشفافية وإخفاء الهوية متى ما كان ذلك مطلوباً نظاماً.

معالجة البيانات الشخصية لمصلحة متحققة

يجوز لجامعة حفر الباطن معالجة البيانات الشخصية دون الاعتماد على موافقة صاحب البيانات متى ما تعذّر الحصول عليها، وذلك إذا كانت المعالجة ضرورية لتحقيق مصلحة متحققة لصاحب البيانات، وبما لا يمس حقوقه أو يسبب له ضرراً، مع الالتزام بتوثيق مبررات المعالجة وفق الضوابط النظامية المعتمدة.

المعالجة لأغراض المصلحة المشروعة

1. يجوز لجامعة حفر الباطن معالجة البيانات الشخصية دون موافقة صاحبها عند وجود مصلحة مشروعة للجامعة، شريطة أن يكون الغرض نظامياً وغير مخالف للأنظمة المعتمدة في المملكة.
2. تلتزم الجامعة بتحقيق التوازن بين المصلحة المشروعة للجامعة وحقوق ومصالح صاحب البيانات الشخصية، مع عدم معالجة البيانات الحساسة إلا وفق الضوابط النظامية.
3. تشمل المصالح المشروعة – على سبيل المثال – حماية الأنظمة والشبكات، وكشف محاولات الاختراق أو الاحتيال، وتعزيز أمن المعلومات واستمرارية الأعمال.

4. قبل البدء في المعالجة، تلتزم الجامعة بإجراء تقييم موثق للمصلحة المشروعة يوضح:
   - الغرض من المعالجة ونوع البيانات المستخدمة.
   - مدى ضرورة المعالجة لتحقيق الغرض.
   - الأثر المحتمل على حقوق أصحاب البيانات والتدابير المتخذة للحد من المخاطر.

5. في حال أظهر التقييم وجود مخاطر جوهرية أو ترتب عليه تغيير في طبيعة المعالجة، تلتزم الجامعة بتعديل المعالجة المقترحة أو الاعتماد على مسوغ نظامي آخر، واتخاذ التدابير اللازمة لتجنب الأضرار المحتملة.

اختيار جهة المعالجة

1. معايير اختيار جهة المعالجة

تلتزم جامعة حفر الباطن عند اختيار جهة لمعالجة البيانات الشخصية بالتحقق من قدرتها على توفير مستوى مناسب من الحماية، وبما يتناسب مع:

- غرض المعالجة وطبيعتها.
- نوع وفئات البيانات الشخصية.
- مدة المعالجة ونطاقها.

2. الالتزام النظامي

يجب أن تتم جميع عمليات المعالجة وفقاً للأنظمة واللوائح المعتمدة في المملكة، دون إخلال بحقوق أصحاب البيانات الشخصية.

3. التعاقد والضوابط

تلتزم الجامعة بإبرام اتفاقيات مكتوبة مع جهات المعالجة تتضمن بوضوح:

- نطاق المعالجة وحدودها.
- التزامات جهة المعالجة بحماية البيانات.
- عدم تنفيذ أي معالجة إضافية إلا بتعليمات مسبقة من الجامعة.

4. الإشراف والمتابعة

تحتفظ الجامعة بحق الإشراف على أعمال جهة المعالجة، والتحقق من التزامها بالضوابط النظامية والتعليمات الصادرة، واتخاذ الإجراءات اللازمة عند وجود أي إخلال.

5. المسؤولية

تظل جامعة حفر الباطن مسؤولة عن حماية البيانات الشخصية ومعالجتها نظاماً، حتى في حال إسناد المعالجة إلى جهة خارجية.

معالجة البيانات الشخصية لغرض آخر غير الذي جُمعت من أجله

1. يجوز لجامعة حفر الباطن معالجة البيانات الشخصية لغرض آخر غير الغرض الأصلي، متى ما كان الغرض الجديد محدداً ومشروعاً ومتوافقاً مع الأحكام النظامية.

2. تلتزم الجامعة قبل البدء بالمعالجة بتوثيق مبررات الغرض الجديد، وتقييم توافقه مع الغرض الأصلي، واتخاذ التدابير اللازمة لحماية البيانات.

3. تُشعر الجامعة صاحب البيانات بالغرض الجديد متى ما كان ذلك مطلوباً نظاماً، وتلتزم بالضوابط الخاصة بالحالات التي تتطلب موافقة.

جمع الحد الأدنى من البيانات الشخصية

1. تلتزم جامعة حفر الباطن بجمع الحد الأدنى الضروري من البيانات الشخصية اللازم لتحقيق الغرض المحدد، وبما يتناسب مع طبيعة الخدمة أو الإجراء.

2. يُحظر جمع بيانات إضافية لا تخدم الغرض المعلن، أو الاحتفاظ ببيانات تتجاوز الحاجة الفعلية للمعالجة.

3. تراجع الجامعة دورياً البيانات المجمعة لضمان تقليلها إلى الحد الأدنى اللازم واستبعاد ما لا يلزم.

الإفصاح عن البيانات الشخصية

1. ضوابط الإفصاح

تلتزم جامعة حفر الباطن بعدم الإفصاح عن البيانات الشخصية إلا لأغراض محددة ومشروعة، وبما يتوافق مع الأحكام النظامية المعتمدة، مع اتخاذ التدابير اللازمة لحماية خصوصية صاحب البيانات.

2. حماية الخصوصية وتقليل البيانات

عند الإفصاح، تلتزم الجامعة بالإفصاح عن الحد الأدنى الضروري من البيانات لتحقيق الغرض، وبما يضمن عدم الإضرار بخصوصية صاحب البيانات أو أي طرف آخر.

3. الإفصاح للجهات العامة

يجوز للجامعة الإفصاح عن البيانات الشخصية للجهات العامة عند وجود مسوغ نظامي، مثل متطلبات السلامة العامة أو تنفيذ الأنظمة أو الأوامر القضائية، مع توثيق طلب الإفصاح والغرض منه.

4. الإفصاح عن بيانات أطراف أخرى

في حال تضمن الإفصاح بيانات شخصية مرتبطة بأشخاص آخرين غير صاحب الطلب، تلتزم الجامعة بموازنة الحقوق، واتخاذ الإجراءات التي تضمن عدم التعرف على الطرف الآخر أو المساس بخصوصيته.

5. التوثيق والمساءلة

تلتزم الجامعة بتوثيق جميع عمليات الإفصاح عن البيانات الشخصية ضمن سجلات المعالجة، بما يشمل الجهة المستفيدة، ونوع البيانات، والغرض من الإفصاح.

ضوابط معالجة البيانات الشخصية لأغراض المصلحة العامة

1. يجوز لجامعة حفر الباطن جمع ومعالجة البيانات الشخصية – سواء من صاحبها مباشرة أو من أطراف أخرى – متى ما كان ذلك ضرورياً لتحقيق مصلحة عامة واضحة ومحددة، وداخلة ضمن اختصاصاتها النظامية.

2. تلتزم الجامعة باتخاذ التدابير التنظيمية والتقنية المناسبة للحد من أي مخاطر محتملة ناتجة عن المعالجة، وبما يضمن حماية حقوق أصحاب البيانات الشخصية.

3. يتم تضمين جميع عمليات المعالجة لأغراض المصلحة العامة ضمن سجلات أنشطة المعالجة، مع الالتزام بجمع الحد الأدنى من البيانات اللازم لتحقيق الغرض.

تصحيح البيانات الشخصية

يحق لصاحب البيانات الشخصية طلب تصحيح بياناته في حال كانت غير دقيقة أو غير مكتملة، وذلك وفق الإجراءات المعتمدة لدى جامعة حفر الباطن.

1. تلتزم الجامعة بما يلي عند تصحيح البيانات:
   - التحقق من دقة البيانات ومراجعة المستندات الداعمة عند الحاجة.
   - إشعار صاحب البيانات بإتمام التصحيح دون تأخير غير مبرر.
   - توثيق جميع التعديلات التي تطرأ على البيانات الشخصية.

2. في حال كانت البيانات محل الطلب قيد المعالجة أو ذات أثر على أطراف أخرى، تلتزم الجامعة باتخاذ الإجراءات اللازمة لضمان عدم الإضرار بحقوق أي طرف.

3. تعتمد الجامعة سياسات وإجراءات داخلية تضمن دقة البيانات الشخصية ومراجعتها بشكل دوري، وتمكين أصحاب البيانات من ممارسة حق التصحيح بسهولة وفاعلية.

أمن المعلومات

تلتزم جامعة حفر الباطن باتخاذ التدابير التنظيمية والإدارية والتقنية اللازمة لحماية أمن البيانات الشخصية وخصوصية أصحابها، وبما يحقق ما يلي:

1. حماية البيانات

تطبيق الضوابط الأمنية المناسبة للحد من مخاطر تسريب أو فقدان أو إساءة استخدام البيانات الشخصية.

2. الالتزام بالمعايير الوطنية

الالتزام بالسياسات والمعايير والضوابط الصادرة عن الجهة الوطنية المختصة بالأمن السيبراني، وتطبيق أفضل الممارسات المعتمدة في هذا المجال.

الإشعار عن حوادث تسريب البيانات الشخصية

1. الإشعار عند حدوث التسريب

تلتزم جامعة حفر الباطن بإشعار صاحب البيانات الشخصية عند وقوع حادثة تسريب لبياناته الشخصية، وذلك خلال مدة لا تتجاوز (72) ساعة من تاريخ علمها بالحادثة، متى ما كان من شأن التسريب الإضرار بحقوقه أو مصالحه.

2. محتوى الإشعار

يجب أن يتضمن الإشعار – بحد أدنى – ما يلي:

- وصف موجز لطبيعة حادثة التسريب ووقت وقوعها.
- نوع البيانات الشخصية المتأثرة.
- الإجراءات المتخذة للحد من آثار التسريب ومنع تكراره.
- وسائل التواصل مع الجهة المختصة أو مسؤول حماية البيانات بالجامعة.

3. الإشعار للجهات المختصة

تلتزم الجامعة بإشعار الجهة المختصة بالأمن السيبراني أو الجهات النظامية ذات العلاقة بحوادث تسريب البيانات، وفق المتطلبات المعتمدة في المملكة.

4. التأخير المبرر في الإشعار

يجوز تأخير إشعار صاحب البيانات إذا كان الإشعار الفوري قد يسبب ضرراً أكبر أو يعرقل إجراءات التحقيق أو المعالجة، على أن يتم الإشعار فور زوال سبب التأخير مع توثيق مبرراته.

5. التوثيق والمتابعة

تلتزم الجامعة بتوثيق جميع حوادث تسريب البيانات الشخصية والإجراءات المتخذة بشأنها، ومتابعة آثارها واتخاذ التدابير اللازمة للحد من المخاطر المستقبلية.

تقييم الأثر على البيانات الشخصية

1. متى يُجرى تقييم الأثر

تلتزم جامعة حفر الباطن بإجراء تقييم أثر قبل البدء في أي معالجة للبيانات الشخصية يُحتمل أن تنطوي على مخاطر على حقوق أو مصالح أصحاب البيانات، وبشكل خاص في الحالات التالية:

- معالجة البيانات الحساسة.
- المعالجة واسعة النطاق أو المتكررة.
- المعالجة التي تعتمد على تقنيات حديثة أو قرارات آلية.

2. محتوى تقييم الأثر

يجب أن يتضمن تقييم الأثر – كحد أدنى – ما يلي:

- وصف طبيعة المعالجة وأغراضها ونطاقها.
- أنواع البيانات الشخصية ومصادرها والفئات المعنية.
- تقييم المخاطر المحتملة على حقوق أصحاب البيانات.
- التدابير التنظيمية والتقنية المتخذة للحد من المخاطر.

3. توثيق ومراجعة التقييم

تحتفظ الجامعة بنسخة موثقة من تقييم الأثر، وتقوم بمراجعته وتحديثه متى ما طرأ تغيير جوهري على طبيعة المعالجة أو مستوى المخاطر.

4. اتخاذ القرار

في حال أظهر تقييم الأثر مخاطر مرتفعة لا يمكن الحد منها بشكل كافٍ، تلتزم الجامعة بتعديل المعالجة أو إيقافها، أو اتخاذ مسوغ نظامي آخر يضمن حماية حقوق أصحاب البيانات الشخصية.

معالجة البيانات الصحية

1. حماية البيانات الصحية

تلتزم جامعة حفر الباطن باتخاذ التدابير التنظيمية والإدارية والتقنية اللازمة لحماية البيانات الصحية والحفاظ على سريتها وخصوصيتها، والحد من الوصول غير المصرح به أو إساءة الاستخدام.

2. الالتزام بالأنظمة والضوابط

تلتزم الجامعة بتطبيق الأنظمة واللوائح والتعليمات الصادرة عن الجهات المختصة بتنظيم القطاع الصحي في المملكة، بما في ذلك متطلبات الأمن الصحي وحماية البيانات الصحية.

3. تحديد المسؤوليات والصلاحيات

يتم تحديد وتوثيق الأدوار والمسؤوليات والصلاحيات المتعلقة بمعالجة البيانات الصحية داخل الجامعة، بما يضمن حصر الوصول على المخولين فقط وفق مبدأ الحاجة إلى المعرفة.

4. توثيق دورة المعالجة

تلتزم الجامعة بتوثيق مراحل معالجة البيانات الصحية وتحديد الجهة أو الشخص المسؤول في كل مرحلة من مراحل المعالجة.

5. الحد الأدنى من البيانات

تقتصر معالجة البيانات الصحية على الحد الأدنى اللازم لتحقيق الغرض الصحي المحدد، وبما يتناسب مع طبيعة الخدمات أو البرامج الصحية المقدمة.

6. إسناد المعالجة

في حال إسناد أي أعمال تتعلق بمعالجة البيانات الصحية إلى جهات خارجية، تلتزم الجامعة بضمان التزام تلك الجهات بالضوابط النظامية والأمنية المعتمدة.

معالجة البيانات الائتمانية

1. تلتزم جامعة حفر الباطن باتخاذ الإجراءات التنظيمية والتقنية اللازمة لحماية البيانات الائتمانية وضمان استخدامها في حدود الأغراض النظامية المحددة.

2. تطبق الجامعة الأنظمة والضوابط الصادرة عن الجهات المختصة بتنظيم المعلومات الائتمانية في المملكة، وتحدد بوضوح مسؤوليات العاملين والجهات ذات العلاقة بمعالجة هذه البيانات.

3. لا تتم معالجة البيانات الائتمانية إلا بعد الحصول على موافقة صريحة من صاحب البيانات، متى ما كانت الموافقة مطلوبة نظاماً، مع توثيقها وفق الإجراءات المعتمدة.

معالجة البيانات لأغراض دعائية أو توعوية

1. يجوز لجامعة حفر الباطن استخدام البيانات الشخصية لأغراض دعائية أو توعوية بعد الحصول على موافقة مسبقة وصريحة من صاحب البيانات، ما لم ينص النظام على خلاف ذلك.

2. يجب أن تكون الموافقة:
   - واضحة ومحددة الغرض.
   - مستقلة عن أي موافقات أخرى.
   - قابلة للإثبات والتوثيق.

3 تلتزم الجامعة بتمكين صاحب البيانات من سحب موافقته في أي وقت، وإيقاف الإرسال الدعائي أو التوعوي فوراً دون تأثير سلبي عليه.

4 تلتزم الجامعة بعدم مشاركة البيانات الشخصية المستخدمة لأغراض دعائية أو توعوية مع أي طرف آخر دون مسوغ نظامي.

5 توضح الجامعة في جميع الرسائل الدعائية أو التوعوية هوية الجهة المرسلة ووسيلة التواصل، مع توفير خيار سهل لإلغاء الاشتراك.

التسويق المباشر

1 تلتزم جامعة حفر الباطن بعدم استخدام البيانات الشخصية لأغراض التسويق المباشر إلا بعد الحصول على موافقة صريحة ومسبقة من صاحب البيانات، وفق الأحكام النظامية المعتمدة.

2 تُمكّن الجامعة صاحب البيانات من إلغاء الاشتراك أو العدول عن موافقته على التسويق المباشر في أي وقت وبوسيلة سهلة وميسّرة.

3 يجب أن تتضمن الرسائل التسويقية هوية الجهة المرسلة ووسيلة واضحة للتواصل أو إيقاف الإرسال.

جمع ومعالجة البيانات لأغراض علمية أو بحثية أو إحصائية

1 يجوز للجامعة جمع ومعالجة البيانات الشخصية لأغراض علمية أو بحثية أو إحصائية دون موافقة صاحب البيانات متى ما تعذر الحصول عليها، وبما لا يؤدي إلى التعرف على هوية صاحب البيانات.

2 تلتزم الجامعة بتطبيق مبدأ تقليل البيانات، واستخدام أساليب إخفاء الهوية أو الترميز كلما أمكن ذلك.

3 تتخذ الجامعة التدابير اللازمة لضمان عدم إلحاق أي ضرر بحقوق أو مصالح أصحاب البيانات الشخصية.

تصوير الوثائق الرسمية التي تحتوي بيانات شخصية

يجوز للجامعة تصوير الوثائق الرسمية التي تحتوي بيانات شخصية دون موافقة صاحبها، متى ما كان ذلك استجابة لطلب جهة عامة مختصة أو تنفيذاً لالتزام نظامي.

1 تقتصر عملية التصوير والمعالجة على الحد الأدنى اللازم لتحقيق الغرض المحدد.

2 تلتزم الجامعة بالحفاظ على سرية الوثائق المصورة وتطبيق الضوابط النظامية المعتمدة لحمايتها.

مسؤول حماية البيانات الشخصية

1 تقوم جامعة حفر الباطن بتعيين مسؤول لحماية البيانات الشخصية في الحالات التي تتطلب ذلك نظاماً، وبما يتناسب مع طبيعة ونطاق أنشطة معالجة البيانات في الجامعة.

2 يكون مسؤول حماية البيانات مختصاً بالإشراف على الالتزام بأحكام حماية البيانات الشخصية داخل الجامعة، ويؤدي مهامه باستقلالية وحياد.

3 تشمل مهام مسؤول حماية البيانات – على سبيل المثال لا الحصر – ما يلي:

- متابعة التزام الجامعة بالأنظمة والسياسات المعتمدة لحماية البيانات الشخصية.
- تقديم المشورة بشأن متطلبات حماية البيانات والممارسات النظامية.
- الإشراف على تقييمات الأثر، ومتابعة ضوابط أمن البيانات، والتقارير ذات العلاقة.
- تمكين أصحاب البيانات من ممارسة حقوقهم، والرد على الطلبات والشكاوى المتعلقة ببياناتهم.
- التنسيق مع الجهات المختصة في حال وقوع حوادث تسريب البيانات الشخصية.

4 تلتزم الجامعة بتوفير الصلاحيات والدعم اللازم لمسؤول حماية البيانات لأداء مهامه بفاعلية، وضمان عدم تعارض مهامه مع أي مسؤوليات أخرى قد تؤثر على استقلاليته.

5 يتم توثيق تعيين مسؤول حماية البيانات وتحديد مهامه وصلاحياته ضمن السياسات والإجراءات الداخلية المعتمدة في الجامعة.

سجلات أنشطة معالجة البيانات الشخصية

1 تلتزم جامعة حفر الباطن بالاحتفاظ بسجلات محدثة لأنشطة معالجة البيانات الشخصية طوال مدة المعالجة، وبما يضمن توثيق جميع العمليات المرتبطة بها.

2 تكون سجلات أنشطة المعالجة مكتوبة ومحدثة ومتاحة للجهات المختصة عند الطلب.

3 تتضمن سجلات المعالجة – كحد أدنى – المعلومات التالية:

- اسم الجهة المعالجة ووسائل التواصل معها.
- أغراض المعالجة وأنواع البيانات الشخصية المعالجة.
- فئات أصحاب البيانات والجهات التي تم الإفصاح لها.
- مدد الاحتفاظ بالبيانات وآليات الإتلاف.
- التدابير التنظيمية والإدارية والتقنية المتخذة لحماية البيانات.

التسجيل في السجل الوطني لمعالجة البيانات الشخصية

تلتزم جامعة حفر الباطن بالتسجيل في السجل الوطني لمعالجة البيانات الشخصية لدى الجهة المختصة، وتحديث بيانات التسجيل وفق المتطلبات النظامية المعتمدة.

جهات إصدار شهادات الاعتماد

تلتزم الجامعة بالتعامل مع جهات إصدار شهادات الاعتماد المعتمدة نظاماً عند الحاجة، وبما يتوافق مع الأحكام والضوابط الصادرة عن الجهات المختصة.

التدقيق والفحص والمراجعة

1 تخضع أنشطة معالجة البيانات الشخصية في الجامعة لعمليات تدقيق وفحص ومراجعة دورية للتحقق من الالتزام بالأنظمة واللوائح المعتمدة.

2 تشمل أعمال المراجعة التحقق من سلامة الإجراءات التنظيمية والتقنية، ومستوى حماية البيانات الشخصية.

3 تلتزم الجامعة بمعالجة أي ملاحظات أو مخالفات يتم رصدها خلال عمليات التدقيق، واتخاذ الإجراءات التصحيحية اللازمة.

تقديم ومعالجة الشكاوى

1 يحق لصاحب البيانات الشخصية التقدم بشكوى إلى الجهة المختصة في الجامعة خلال مدة لا تتجاوز (90) يوماً من تاريخ علمه بالحادثة محل الشكوى، ويجوز قبول الشكوى بعد هذه المدة في الحالات المبررة.

2 يتولى مكتب إدارة البيانات بالجامعة استقبال الشكاوى عبر القنوات المعتمدة، والتحقق منها، ودراستها، واتخاذ الإجراءات اللازمة لمعالجتها خلال مدة مناسبة، مع إشعار مقدم الشكوى بالنتيجة.

3 يجب أن تتضمن الشكوى – كحد أدنى – البيانات التالية:

- بيانات مقدم الشكوى ووسائل التواصل معه.
- وصف واضح لموضوع الشكوى ووقائعها.
- أي مستندات أو معلومات داعمة.

4 تلتزم الجامعة بتوثيق الشكاوى والإجراءات المتخذة بشأنها، وطلب ما يلزم من معلومات إضافية عند الحاجة.

نشر السياسة

تلتزم جامعة حفر الباطن بنشر سياسة حماية البيانات الشخصية في القنوات الرسمية المعتمدة لديها، والعمل بها من تاريخ اعتمادها، بما يضمن إطلاع أصحاب البيانات والجهات ذات العلاقة على أحكامها.

خامسًا

الأدوار والمسؤوليات

مجلس الجامعة / الإدارة العليا

- اعتماد سياسة حماية البيانات الشخصية.
- دعم تطبيق السياسة وتوفير الموارد اللازمة.
- الإشراف العام على الالتزام النظامي.

رئيس الجامعة

- توجيه الجهات ذات العلاقة بتطبيق السياسة.
- ضمان الالتزام بأحكام نظام حماية البيانات الشخصية واللوائح ذات الصلة.

مكتب إدارة البيانات

- الإشراف على تطبيق سياسة حماية البيانات الشخصية.
- إعداد وتحديث السياسات والإجراءات المرتبطة بحماية البيانات.
- متابعة الامتثال والتنسيق مع الجهات الداخلية والخارجية.

مسؤول حماية البيانات الشخصية (DPO)

- مراقبة الالتزام بأحكام نظام حماية البيانات الشخصية.
- تقديم الاستشارات الفنية والتنظيمية.
- الإشراف على تقييمات الأثر وسجلات المعالجة.
- التعامل مع طلبات أصحاب البيانات والشكاوى.
- التنسيق في حالات تسريب البيانات.

عمادة التعليم الإلكتروني والتحول الرقمي

- تطبيق الضوابط التقنية والتنظيمية لحماية البيانات الشخصية في الأنظمة والمنصات الرقمية.
- إدارة الوصول والصلاحيات للأنظمة التعليمية والإدارية.
- دعم الاستجابة للحوادث الرقمية وتسريب البيانات الشخصية بالتنسيق مع الجهات المختصة.

الأمن السيبراني

- تطبيق سياسات وضوابط الأمن السيبراني المعتمدة.
- تقييم المخاطر الأمنية المرتبطة بالبيانات الشخصية.
- المشاركة في التحقيق بحوادث الاختراق أو التسريب.

الجهات المالكة للبيانات (Data Owners)

- تحديد أغراض المعالجة وحدودها.
- ضمان دقة البيانات وصحتها.
- الموافقة على الإفصاح أو مشاركة البيانات وفق السياسة.

الجهات المعالجة للبيانات (Data Processors)

- معالجة البيانات الشخصية وفق تعليمات الجامعة فقط.
- الالتزام بالضوابط الأمنية والتنظيمية.
- عدم استخدام البيانات لأي غرض آخر.

الموظفون ومنسوبو الجامعة

- الالتزام بسياسة حماية البيانات الشخصية.
- حماية البيانات التي يطلعون عليها بحكم العمل.
- الإبلاغ عن أي حادثة تسريب أو مخالفة.

الجهات الخارجية المتعاقدة

- الالتزام باتفاقيات معالجة البيانات.
- تطبيق ضوابط الحماية والسرية.
- التعاون مع الجامعة في حالات التدقيق أو الحوادث.

أصحاب البيانات الشخصية

- ممارسة حقوقهم النظامية (الاطلاع، التصحيح، الحذف، الاعتراض...).
- تقديم الطلبات أو الشكاوى عبر القنوات المعتمدة.

بيانات التواصل

يمكن التواصل مع مكتب إدارة البيانات من خلال البريد الالكتروني dmo@uhb.edu.sa

الوثائق ذات العلاقة

- سياسة خصوصية واستخدام البيانات
- وثيقة إدارة التعامل مع تسريب البيانات.
- نظام حماية البيانات الشخصية – مكتب إدارة البيانات الوطنية
- سياسة الاستخدام الأخلاقي للذكاء الاصطناعي-الهيئة السعودية للبيانات والذكاء الاصطناعي

المراجع

نظام حماية البيانات الشخصية ولوائحه التنظيمية

https://sdaia.gov.sa/ar/SDAIA/about/Documents/ImplementingRegulationPersonalDataProtectionLawAr.pdf