DATENSCHUTZERKLÄRUNG VON TIDEWATCH

TideWatch Partners, LLC („TideWatch“) ist Eigentümer und Administrator von tidewatch.com. TideWatch verpflichtet sich, die Privatsphäre und Sicherheit der Benutzer zu schützen. TideWatch erläutert mit dieser Datenschutzerklärung seine PraxisPraxis in Bezug auf die Erhebung und Weitergabe von Informationen. Diese Datenschutzerklärung gilt nur für Informationen, die auf der Website tidewatch.com (die „Website“) gesammelt werden. Bitte lesen Sie diese Anleitung sorgfältig durch. Mit Ihrem Besuch auf der Website von TideWatch akzeptieren Sie die in dieser Datenschutzerklärung beschriebenen Praxis.

Informationen, die TideWatch gegebenenfalls sammelt

Wenn Sie auf diese Website zugreifen, empfängt TideWatch Informationen von Ihrem Browser und speichert gegebenenfalls Ihre IP-Adresse, die Uhrzeit, verschiedene technische Informationen sowie Informationen über die von Ihnen aufgerufene Seite. Diese Daten offenbaren nicht Ihren Namen oder Ihre persönliche Identität. Sie bleiben anonym.

Wir haben derzeit nicht die Absicht, Ihre personenbezogenen Daten in einer anderen als der zum Zeitpunkt der Erfassung angegebenen Weise zu verwenden. Wenn wir Ihre personenbezogenen Daten jedoch in der Zukunft doch in einer anderen als der zum Zeitpunkt der Erfassung angegebenen Weise verwenden wollen, werden wir diese Datenschutzerklärung entsprechend überarbeiten, und Sie können darüber entscheiden, ob wir Ihre Daten auch auf diese andere Weise nutzen dürfen.

Datenschutzpraxis von Drittenen

Die Website von TideWatch kann Links zu Websites von Dritten enthalten, die Waren, Dienstleistungen oder Informationen anbieten. TideWatch ist nicht verantwortlich für den Inhalt, die Datenschutzerklärungen oder -Praxis von Inserenten oder von verlinkten Websites Dritter. TideWatch fordert Sie dazu auf, die Datenschutzerklärungen solcher Dritter zu überprüfen, bevor Sie ihnen Informationen bereitstellen. Dritte sammeln und verwenden Ihre Daten gegebenenfalls auf andere Weise als in dieser Datenschutzerklärung angegeben.

Änderungen der Datenschutzerklärung

TideWatch behält sich das Recht vor, die Bestimmungen dieser Datenschutzerklärung nach eigenem Ermessen und jederzeit, sei es mit oder ohne Ankündigung, zu ergänzen oder anderweitig zu ändern. Falls dies gesetzlich vorgeschrieben ist, wird TideWatch die neue Datenschutzerklärung auf seiner Website veröffentlichen und/oder Ihnen eine Mitteilung über die Änderung gemäß dem/den gesetzlich geltenden Verfahren senden. Wenn Sie im Anschluss an eine solche Mitteilung weiterhin die Dienstleistungen von TideWatch oder sonstige Dienstleistungen nutzen, so stimmen Sie damit der überarbeiteten Datenschutzerklärung zu.

Fragen

Sollten Sie Fragen zu dieser Datenschutzerklärung haben, kontaktieren Sie uns bitte unter der Rufnummer +1 (603) 559-9999, senden Sie eine E-Mail an t w p @ t i d e w a t c h . c o m oder schreiben Sie uns unter folgender Adresse: TideWatch, Attn.: Director of Information Privacy, PO Box 219, Greenland, NH 03840 (USA).

DATENSCHUTZERKLÄRUNG FÜR DIE MARKTFORSCHUNG

TideWatch Partners, LLC („TideWatch“) ist ein Marktforschungsunternehmen, das sich verpflichtet, die Privatsphäre und die Sicherheit personenbezogener Daten zu wahren. TideWatch handelt nach den Grundsätzen des mandatierten Normen- und Ethikkodex für die Meinungsforschung des Marktforschungsverbandes MRA. Dieser Kodex enthält Anforderungen in Bezug auf den Schutz personenbezogener Daten sowie auf Informationen, die die Identifizierung von Befragten ermöglichen. Eine Kopie dieses Kodex finden Sie unter http://www.mra-net.org/

Alle Antworten der Teilnehmer werden streng vertraulich behandelt und nur in aggregierter Form – also als Informationen über Gruppen und nicht über Individuen – ausgewiesen, sofern nichts anderes aus der Befragung hervorgeht. Wenn wir angeben, dass in den Forschungsergebnissen gegebenenfalls personenbezogene Daten enthalten sind, garantieren wir, dass diese Informationen streng vertraulich behandelt werden. Wir werden die Teilnehmer in Bezug auf die Art der Forschung und der Datennutzung nicht irreführen. Weitere Informationen finden Sie im nachstehenden Abschnitt „Offenlegung personenbezogener Daten“.

Personenbezogene Daten werden ohne vorherige Zustimmung der Person, die diese Daten bereitgestellt hat, weder durch Verkauf noch Tausch an andere Personen oder Unternehmen weitergegeben. Wir betreiben weder Verkäufe noch Direktmarketing und stellen personenbezogene Daten nicht für Direktverkaufs- oder Marketingzwecke zur Verfügung. Weitere Informationen zu unserem Unternehmen finden Sie auf unserer Website www.tidewatch.com.

Offenlegung personenbezogener Daten

TideWatch begrenzt die Weitergabe persönlich identifizierbarer Daten mit seinen Kunden auf das für das Forschungsprojekt wesentliche Maß. Nachnamen, Telefonnummern und Adressen werden nicht mit Kunden oder sonstigen Dritten geteilt – es sei denn, Projektarbeiten oder Validierungen im Vorfeld der Untersuchung erfordern dies.

Personenbezogene Daten dürfen nur dann offengelegt werden, wenn aus dem Erhebungsinstrument für den jeweiligen Teilnehmer eindeutig hervorgeht, dass die Daten offengelegt werden, oder wenn ein Teilnehmer während der Erhebung eine Frage äußert, die nur durch die Offenlegung von Daten aus der Erhebung beantwortet werden kann.

TideWatch behält sich das Recht vor, persönlich identifizierbare Daten im Zuge einer gesetzlichen Anforderung oder eines Gerichtsbeschlusses offenzulegen; eine entsprechende Mitteilung ist möglicherweise nicht erforderlich.

Im Falle eines Verkaufs, einer Fusion, Liquidation, Auflösung, Reorganisation oder eines Erwerbs von TideWatch wird der Erwerber verpflichtet, sämtliche wesentlichen Bestimmungen dieser Datenschutzerklärung zu erfüllen, bevor wir Informationen an diese Gesellschaft übertragen.

E-Mail-Adressen und sonstige Kommunikation

TideWatch verfügt gegebenenfalls über persönliche E-Mail-Adressen und Telefonnummern in seinem E-Mail-System sowie über Datendateien, die wie folgt zu TideWatch gelangten:

- Informationsanfrage auf unserer Website
- E-Mail-Adressen/Telefonnummern, die an TideWatch geschickt wurden

• Für TideWatch fertiggestellte Forschungsumfragen
• Kunden, die E-Mail-Adressen/Telefonnummern zu Forschungszwecken zur Verfügung gestellt haben

Da TideWatch keine E-Mails zu Verkaufs- oder Direktmarketingzwecken versendet, gilt der CAN-SPAM Act aus dem Jahr 2003 nicht für unsere E-Mail-Kommunikation. Allerdings hält sich TideWatch in Bezug auf die Marktforschung freiwillig an den CAN-SPAM Act. TideWatch nutzt E-Mail als Mittel der Kommunikation mit bekannten Kunden und Forschungsteilnehmern.

Wenn TideWatch potenzielle Teilnehmer per E-Mail zur Mitwirkung an einem Meinungs- und Marktforschungsvorhaben einlädt, hält es sich an die nachstehenden Richtlinien.

- TideWatch identifiziert sich eindeutig als Absender der E-Mail.
- TideWatch stellt dem E-Mail-Empfänger entsprechende Kontaktinformationen für den Fall bereit, dass dieser sich bei Fragen oder Bedenken an TideWatch wenden möchte.
- TideWatch bietet die Möglichkeit an, vom Empfang zusätzlicher E-Mail-Einladungen zwecks Teilnahme an Forschungsprojekten ausgenommen zu werden.
- TideWatch verwendet E-Mail-Adressen nur dann weiter, wenn sie für legitime Folgemails der Umfrageforschung verwendet werden.

COPPA

Wir verpflichten uns zum Schutz der Online-Privatsphäre Ihres Kindes. Deshalb steht unsere Praxis in voller Übereinstimmung mit dem *Children's Online Privacy Protection Act* (COPPA), so wie dies von der FTC (*Federal Trade Commission*) vorgesehen ist. Dies bedeutet, dass TideWatch keine Forschung mit Minderjährigen unter 13 Jahren ohne eine Erlaubniserklärung der Eltern oder Erziehungsberechtigten betreibt. Mehr Informationen zu COPPA finden Sie auf http://www.ftc.gov/ogc/coppa1.htm.

Fragen und Bedenken

Bei weitergehenden Bedenken oder Fragen zu unserer Datenschutzpolitik können Sie uns eine E-Mail an t w p @ t i d e w a t c h . c o m senden oder anrufen: +1 (603) 559–9999.

Rechtliche Hinweise

TideWatch kann personenbezogene Daten gegebenenfalls offenlegen, wenn dies gesetzlich vorgeschrieben ist oder wenn dies im guten Glauben geschieht, dass dies zwecks Übereinstimmung mit den Gesetzen oder im Rahmen eines gerichtlichen Verfahrens erforderlich ist.

Änderungen und Aktualisierungen der Datenschutzerklärung

TideWatch behält sich im Zuge der stetigen Verbesserung aufgrund neuer Technologien das Recht vor, diese Datenschutzerklärung jederzeit zu ändern. Daher empfehlen wir Ihnen, diese Datenschutzerklärung regelmäßig aufzurufen. Wenn wir wesentliche Änderungen an dieser Richtlinie vornehmen, werden wir das auf www.tidewatch.com bekanntgeben.

PROGRAMM FÜR INFORMATIONSSICHERHEIT

TideWatch Partners, LLC (die „Gesellschaft“) hat das nachstehende Programm für Informationssicherheit („Programm“) entwickelt. Mit sofortiger Wirkung unterliegen alle Mitarbeiter und alle unabhängigen Auftragnehmer diesem Programm. Jeder Mitarbeiter und jeder unabhängige Auftragnehmer, der von der Gesellschaft nach dem 1. Oktober 2011 eingestellt bzw. beauftragt wird, erhält eine Kopie des Programms im Rahmen des Orientierungsprozesses.

Für die Zwecke dieses Programms bedeutet „personenbezogene Daten“: Vor- und Nachname oder Anfangsbuchstabe des Vornamens und Nachname einer Person in Kombination mit einer oder mehreren der folgenden Angaben, die sich auf diese Person beziehen: (a) Sozialversicherungsnummer, (b) Führerscheinnummer oder Personalausweis-Nummer , (c) Bankkontonummer oder Kredit- bzw. Debitkartennummer, mit oder ohne erforderlichen Sicherheitscode, Zugangscode, persönliche Identifikationsnummer oder Passwort, wodurch der Zugang zum Bankkonto einer Person ermöglicht würde, (d) medizinische Daten, (e) Krankenversicherungsdaten oder (f) Anschrift, Telefonnummer oder Postleitzahl, jedoch unter der Voraussetzung, dass personenbezogene Daten keine Informationen enthalten dürfen, die rechtmäßig erlangt wurden aus öffentlich zugänglichen Daten bzw. aus Bundes-, Landes- oder Gemeindeverwaltungsakten, die rechtmäßig für die breite Öffentlichkeit zur Verfügung gestellt wurden. Für die Zwecke dieses Programms bedeutet „medizinische Daten“: sämtliche Informationen in Bezug auf die Krankengeschichte einer Person, auf ihre geistige oder körperliche Verfassung, medizinische Behandlung oder Diagnose durch Angehörige eines Gesundheitsberufes; „Krankenversicherungsdaten“ bedeutet: Krankenversicherungsnummer bzw. Mitgliedskennung einer Person, eindeutige Kennung eines Krankenversicherers zur Identifizierung einer Person oder Daten aus der Anwendungs- und Vorgeschichte einschließlich etwaiger Beschwerdeakten.

Das Programm ist staatsunabhängig und bezieht sich auf sämtliche personenbezogenen Daten, die die Gesellschaft erhält, pflegt, verarbeitet oder auf die sie auf sonstige Weise Zugriff hat im Zusammenhang mit der Bereitstellung von Waren oder Dienstleistungen oder im Zusammenhang mit Beschäftigungsverhältnissen.

I. PROGRAMMZIELE

A. Entwicklung von wirksamen administrativen, technischen und physischen Sicherheitsmaßnahmen zum Schutz personenbezogener Daten.

B. Beschreibung der Verfahren zur Bewertung unserer elektronischen und physikalischen Methoden des Zugriffs, der Erfassung, Speicherung, Verwendung, Übertragung und des Schutzes personenbezogener Daten.

C. Gewährleistung von Sicherheit und Vertraulichkeit in Bezug auf personenbezogene Daten.

D. Schutz vor zu erwartenden Bedrohungen oder Gefahren für die Sicherheit und/oder Integrität von personenbezogenen Daten.

E. Schutz vor unbefugtem Zugriff auf oder Verwendung solcher Daten in einer Weise, die ein erhebliches Risiko bezüglich Identitätsdiebstahl oder Betrug darstellt.

II. KOORDINATOR FÜR DATENSICHERHEIT

Die designierte Koordinatorin für Datensicherheit („Koordinator“) der Gesellschaft ist Kristine Campel, Controllerin. Der Koordinator trägt die Verantwortung für folgende Aufgaben:

- Umsetzung des Programms
- Durchführung von Risikobewertungen des Programms, soweit erforderlich
- Konzeption und Durchführung von Schulungen (soweit erforderlich) für diejenigen Personen, die Zugang zu personenbezogenen Daten haben, mit dem Ziel, die Programmvorgaben umzusetzen
- Bewertung von Drittanbietern der Gesellschaft im Hinblick auf ihre Fähigkeit, Sicherheitsmaßnahmen für personenbezogene Daten, die die Gesellschaft ihnen zugänglich gemacht hat, umzusetzen und aufrechtzuerhalten, sowie die Vereinfachung von Verträgen mit solchen Drittanbietern zwecks Umsetzung und Aufrechterhaltung von Sicherheitsmaßnahmen für personenbezogene Daten
- Zusammenarbeit mit IT-Profis zwecks Implementierung der technischen Aspekte des Programms
- Überprüfung des Anwendungsbereichs der aufgeführten Sicherheitsmaßnahmen mindestens einmal pro Jahr oder im Zuge einer wesentlichen Änderung der GeschäftsPraxis
- Durchführung einer jährlichen Schulung für alle Eigentümer, Manager, Mitarbeiter und unabhängigen Auftragnehmer einschließlich der Leih- und Zeitarbeitskräfte, die Zugang zu personenbezogenen Informationen über die Bestandteile des Programms haben. Die Teilnehmer der Schulungen sind verpflichtet, ihre Teilnahme an der Schulung sowie ihre Kenntnisse über die Anforderungen der Gesellschaft im Hinblick auf die Gewährleistung des Schutzes personenbezogener Daten nachzuweisen.
- Sicherstellen, dass die entsprechenden Aufsichts- oder Prüfverfahren zwecks Erfassung der missbräuchlichen Offenlegung oder des Diebstahls personenbezogener Daten vorhanden sind

III. RISIKOBEWERTUNG

Der Koordinator führt, soweit erforderlich, Risikobewertungen durch, die zum Ziel haben, die nach vernünftigem Ermessen vorhersehbaren internen und externen Gefahren für die Sicherheit, Vertraulichkeit und Integrität personenbezogener Daten zu identifizieren, die zu unbefugter Offenlegung, Missbrauch, Veränderung, Zerstörung oder anderweitiger Kompromittierung führen könnten; außerdem bewertet er die Hinlänglichkeit von vorhandenen Sicherheitsvorkehrungen im Hinblick auf die Kontrolle der genannten Risiken.

Der Koordinator legt fest, welche Geschäftsbereiche der Gesellschaft relevant sind für die Risikobewertungen. Mindestens jedoch fallen die folgenden Aspekte unter die Risikobewertung:

- Schulung und Führung der Mitarbeiter
- Informationssysteme, einschließlich Netzwerk- und Software-Design, sowie die Verarbeitung, Speicherung, Übertragung und Vernichtung von Daten
- Erkennung und Vorbeugung von sowie Reaktion auf Cyberangriffe, Eindringlinge oder andere Systemausfälle.

Sobald der Koordinator die nach vernünftigem Ermessen vorhersehbaren Risiken für die personenbezogenen Daten der Gesellschaft identifiziert hat, entscheidet er, ob die diesbezüglichen aktuellen Richtlinien und Verfahren der Gesellschaft die potenziellen Risiken ausreichend eindämmen. Ist dies nicht der Fall, ändert der Koordinator die Richtlinien und Verfahren dahingehend, dass die Vorgaben des Programms erfüllt werden.

IV. REGELMÄSSIGE NEUBEWERTUNG

Der Koordinator kann das Programm nach eigenem Ermessen von Zeit zu Zeit neu bewerten und abändern. Eine solche Neubewertung und Änderung erfolgt auf Basis nachstehender Aspekte:

- Ergebnisse der Prüfungs- und Überwachungsbemühungen im Rahmen des Programms
- Wesentliche Änderungen im Hinblick auf Geschäftstätigkeiten oder -verbindungen bzw. auf die informationstechnologischen Strukturen
- Jeder andere Umstand, der nach Kenntnis des Koordinators einen wesentlichen Einfluss auf das Programm hat.

Um den Koordinator in dieser Hinsicht zu unterstützen, halten die Mitarbeiter ihn über Art und Umfang sämtlicher Beziehungen zu Dritten sowie über etwaige betriebliche Veränderungen oder andere Angelegenheiten, die sich auf die Sicherheit und Integrität der personenbezogenen Daten der Gesellschaft auswirken können, auf dem Laufenden.

V. SCHULUNG UND FÜHRUNG DER MITARBEITER

Im Einklang mit den Zielen des Programms wird die Gesellschaft die folgenden Sicherungsmaßnahmen zur Führung und Schulung der Mitarbeiter anwenden, aufrechterhalten und durchsetzen:

1. Alle Mitarbeiter und unabhängigen Auftragnehmer sind für die Einhaltung dieses Programms verantwortlich.

2. Alle neuen Mitarbeiter und unabhängigen Auftragnehmer, die Dienstleistungen für die Gesellschaft erbringen und Zugang zu personenbezogenen Daten haben, nehmen am Informationssicherheitstraining der Gesellschaft teil. Jede Person bestätigt ihr Einverständnis, was die Einhaltung des Programms der Gesellschaft betrifft. Als Mindestvoraussetzung umfasst das Schulungsprogramm grundlegende Schritte zur Aufrechterhaltung der Sicherheit, Vertraulichkeit und Integrität personenbezogener Daten, wie zum Beispiel:

    - Mitarbeitern und unabhängigen Auftragnehmern aufzeigen, welche Arten von personenbezogenen Daten als schutzwürdig im Rahmen dieses Programms gelten
    - Prüfung und Erörterung des Programms
    - Angemessene Sicherung des physischen Standorts von personenbezogenen Daten einschließlich verschließbarer Räume oder Aktenschränke (soweit angemessen) sowie die sichere Aufbewahrung von Schlüsseln und Codes
    - Verwendung passwortgeschützter Computersoftware, -systeme, -anwendungen oder -terminals oder einer automatischen Abmeldefunktion, die den Zugriff nach kurzer Inaktivität beendet
    - Verwendung geeigneter Passwörter
    - Regelmäßige Änderung und Aufrechterhaltung der Sicherheit von Passwörtern
    - Angemessene Sicherung der elektronischen Übermittlung personenbezogener Daten
    - Geeignete Vernichtung von gedruckten und elektronischen Aufzeichnungen
    - Sonstige Schulungen, die das Management von Zeit zu Zeit als angemessen erachtet

3. Die Gesellschaft unternimmt geeignete Schritte, um das Bewusstsein für und die Einhaltung des Programms zu fördern.

4. Alle Mitarbeiter und unabhängigen Auftragnehmer sind nach Festlegung der Gesellschaft berechtigt, gemäß dem Need-to-know-Prinzip auf personenbezogene Daten zuzugreifen.

5. Der Zugriff, die Nutzung oder Vervielfältigung von personenbezogenen Daten (sei es in elektronischer oder nicht-elektronischer Form) durch das Personal für den eigenen Gebrauch oder für eine von der Gesellschaft nicht autorisierte Nutzung ist nicht erlaubt.

6. Personen, die dieses Programm nicht einhalten, unterliegen Disziplinarmaßnahmen bis hin zur Kündigung des Arbeitsverhältnisses für Mitarbeiter oder Vertragsbeendigung für unabhängige Vertragspartner, die Dienstleistungen für die Gesellschaft erbringen.

VI. SICHERUNGSMASSNAHMEN FÜR INFORMATIONSSYSTEME

Im Einklang mit den Zielen des Programms wird die Gesellschaft die folgenden Sicherungsmaßnahmen für Informationssysteme anwenden, aufrechterhalten und durchsetzen, sowie sich nach Bedarf von IT-Profis beraten lassen:

A. Papieraufzeichnungen

1. Papier- oder elektronische Aufzeichnungen, die personenbezogene Daten enthalten, werden in gesicherten Bereichen gespeichert und aufbewahrt. Der Koordinator kontrolliert den Zugang zu diesen Bereichen. Mitarbeiter, die Schlüssel oder Sperrcodes zu solchen Aufzeichnungen besitzen, sind verpflichtet, diese Schlüssel und Codes nach Anweisung des Koordinators oder Abteilungsleiters sicher aufzubewahren.

2. Papieraufzeichnungen, die personenbezogene Daten enthalten, dürfen niemals unbeaufsichtigt in einem nicht gesicherten Bereich verbleiben.

3. Abgelegte Papieraufzeichnungen, die personenbezogene Daten enthalten, müssen in verschlossenen und gesicherten Behältern aufbewahrt werden; sobald sie nicht mehr benötigt werden, müssen sie geschreddert oder in anderer geeigneter Weise vernichtet werden.

4. Papieraufzeichnungen, die personenbezogene Daten enthalten, werden sachgerecht vernichtet, sobald die Gesellschaft keinen Bedarf mehr an der Aufbewahrung dieser Daten hat.

B. Elektronische Aufzeichnungen

1. Der Koordinator sorgt in Verbindung mit IT-Profis dafür, dass die Gesellschaft die für den Schutz personenbezogener Daten technisch erforderlichen Anlagen einsetzt und instand hält.

2. Der Koordinator sorgt in Verbindung mit IT-Profis dafür, dass der erforderliche Austausch mit den Computerlieferanten der Gesellschaft stattfindet, damit gewährleistet ist, dass die Gesellschaft mit der jeweils aktuellsten Korrektursoftware zur Behebung potenzieller Sicherheitslücken in der Software ausgestattet ist.

3. Der Koordinator sorgt in Verbindung mit IT-Profis dafür, dass die Gesellschaft Verfahren zur Aufrechterhaltung der Sicherheit, Vertraulichkeit und Integrität personenbezogener Daten für den Fall entwickelt, dass ein Computerausfall oder ein anderes technisches Versagen eintritt.

4. Elektronische personenbezogene Daten müssen auf sicheren Netzwerkservern der Gesellschaft gespeichert werden.

5. Die Gesellschaft fordert dazu auf, eingehende Übertragungen von personenbezogenen Daten aus anderen Quellen an die Gesellschaft zu verschlüsseln oder anderweitig zu sichern.

6. Ausgehende Übertragungen von personenbezogenen Daten müssen auf einem angemessenen Sicherheitsniveau erfolgen und in einer für den Koordinator akzeptablen Weise gesichert werden.

7. Festplatten, Disketten, Magnetbänder oder sonstige elektronische Medien, die personenbezogene Daten enthalten, werden vor der Entsorgung von Computern oder anderer Hardware gelöscht und/oder zerstört; dies erfolgt so oft wie nach Festlegung des Koordinators erforderlich.

8. Der Koordinator betreibt eine rollierende Inventur der Firmencomputer, einschließlich Laptops und Handheld-Geräte oder PDAs, auf und mit denen personenbezogene Daten gespeichert, abgerufen und übertragen werden können, um sicherzustellen, dass diese Geräte die notwendige Technologie zur Sicherung der Übertragung von personenbezogenen Daten enthalten.

9. Die Gesellschaft verwendet ein Antivirenprogramm, das regelmäßig aktualisiert wird.

10. Die Gesellschaft verwendet und unterhält eine Firewall-Konfiguration zum Schutz von Benutzerkontendaten.

11. Die Gesellschaft regelt den Zugriff auf elektronische personenbezogene Daten über eine Benutzeridentifikation, die für den Zugriff auf das Computernetzwerk der Gesellschaft erforderlich ist.

12. Die Gesellschaft regelt den Zugriff auf elektronische personenbezogene Daten, indem sie Personen, die berechtigt sind, personenbezogene Daten abzurufen, eindeutige Benutzerkennungen und Passwörter zuweist, die so konzipiert sind, dass die Sicherheit dieser Zugangskontrollen aufrechterhalten wird.

13. Die Gesellschaft verwendet keine Herstellervorgaben für Systemkennwörter und andere Sicherheitsparameter.

14. Mitarbeiter und unabhängige Auftragnehmer müssen (a) Passwörter auf Computer- und Elektroniksystemen der Gesellschaft stets auf die autorisierte Art und Weise verwenden, (b) passwortgeschützte Bereiche auf Computer- und Elektroniksystemen der Gesellschaft respektieren,

(c) Passwörter geheim halten und sicher aufbewahren und (d) ihr Passwort routinemäßig ändern. Die Mitarbeiter dürfen jedoch die Maßnahmen zum Passwortschutz nicht dazu verwenden, autorisierte Vertreter der Gesellschaft (z. B. den Koordinator oder das IT-Personal) am Zugang zu den Computer- und Elektroniksystemen der Gesellschaft zu hindern.

15. Die Gesellschaft blockiert den Zugriff auf elektronische Aufzeichnungen nach mehreren erfolglosen Zugriffsversuchen.

16. Mitarbeiter und unabhängige Auftragnehmer werden im Hinblick auf die richtige Benutzung des Computersicherheitssystems und die Bedeutung der Sicherheit personenbezogener Daten geschult.

17. Beendet ein Mitarbeiter oder Lieferant seine Tätigkeit für die Gesellschaft, schränkt die Gesellschaft umgehend deren Zugriff auf personenbezogene Daten ein und verlangt die sofortige Rückgabe aller Aufzeichnungen, die personenbezogene Daten enthalten und zum Zeitpunkt der Kündigung/Beendigung gegebenenfalls im Besitz des ehemaligen Mitarbeiters oder Lieferanten waren.

VII. BENACHRICHTIGUNG BEI DATENSCHUTZVERLETZUNGEN

A. Datenschutzverletzungen

Der Koordinator benachrichtigt Einzelpersonen, wenn eine „Verletzung der Sicherheit“ von personenbezogenen Daten vorliegt. Eine „Verletzung der Sicherheit“ ist die unberechtigte Übernahme oder unbefugte Nutzung von: (1) unverschlüsselten personenbezogenen Daten oder verschlüsselten elektronischen personenbezogenen Daten und des vertraulichen Prozesses oder Schlüssels, der die Sicherheit, Vertraulichkeit oder Integrität der personenbezogenen Daten kompromittieren kann, was ein erhebliches Risiko bezüglich Identitätsdiebstahl oder Betrug darstellt. Eine gutgläubige, aber unbefugte Übernahme von personenbezogenen Daten durch einen Mitarbeiter oder Vertreter der Gesellschaft für rechtmäßige Zwecke dieses Mitarbeiters oder Vertreters stellt keine Verletzung der Sicherheit dar, es sei denn, die personenbezogenen Daten werden unberechtigt verwendet oder sind Gegenstand weiterer unbefugter Offenlegungen.

Der Koordinator benachrichtigt auch den jeweiligen Besitzer der Daten oder Lizenznehmer, wenn eine „Verletzung der Sicherheit“ von personenbezogenen Daten vorliegt, die nicht im Besitz der Gesellschaft sind.

Jeder, der diesem Programm unterliegt, muss umgehend den Koordinator benachrichtigen, wenn er Kenntnis von oder Grund zur Annahme einer Verletzung der Sicherheit hat.

B. Benachrichtigung

Der Koordinator koordiniert die Benachrichtigungen von Personen, die Gegenstand einer Datenschutzverletzung gemäß den am Wohnort der Person geltenden bundes- oder einzelstaatlichen Gesetzen oder Vorschriften stehen. Die Benachrichtigung sollte zumindest Folgendes beinhalten: (1) eine Beschreibung der Art und Umstände der Sicherheitsverletzung, des unerlaubten Erwerbs oder der Nutzung personenbezogener Daten, (2) die diesbezüglich bereits getroffenen oder geplanten

Maßnahmen und (3) eine Information darüber, ob Strafverfolgungsbehörden in die Untersuchung des Vorfalls einbezogen wurden.

C. Briefing nach der Sicherheitsverletzung

Im Falle einer Datensicherheitsverletzung ist der Koordinator zuständig für die Beurteilung der Sicherheitsverletzung, was auch die von der Verletzung betroffenen Personen mit einschließt. Die Beurteilung umfasst die Erörterung der Art der Sicherheitsverletzung, die getroffenen Korrekturmaßnahmen sowie gegebenenfalls die Änderung des Programms zwecks Verbesserung der Sicherheit.

VIII. DRITTANBIETER

Der Koordinator hat Drittanbieter identifiziert, die Zugriff auf mit der Gesellschaft verbundene personenbezogene Daten haben. Die Gesellschaft hat jeden Drittanbieter aufgefordert, der Gesellschaft seine Datenschutzerklärung und -verfahren vorzulegen, damit ein angemessener Schutz von personenbezogenen Daten im Einklang mit diesem Programm gewährleistet ist.

Alle nach dem 1. März 2010 mit einem Drittanbieter eingegangenen Verträge enthalten eine Bestimmung, die von Drittanbietern verlangt, geeignete Sicherheitsmaßnahmen zu umzusetzen und aufrechtzuerhalten, damit personenbezogene Daten, die die Gesellschaft mit Drittanbietern austauscht, geschützt werden.

DATENSCHUTZERKLÄRUNG FÜR DEN KUNDENBEREICH

Unsere Datenschutzerklärung im Hinblick auf Daten, die in unserem „Kunden-Login“-Bereich erfasst werden, finden Sie unter folgendem Link:
https://www.tidewatch.com/clientlogin/images/stories/clientlogin_privacy.pdf