WELL 1-2-1 GDPR COMPLIANCE

V101

WELLBEING4BUSINESS LTD

2/23/2018

ABOUT THE APP

WELL121 is a health tracking app that links, through consent to an online health coach. The WELL121 APP has been approved by both APPLE and GOOGLE and is available to download freely. The app uses the world reknown Nudge software which has been customised and branded by Wellbeing4business Ltd for distribution

WELL 121 can be:

- Used by individuals who download the app
- Used by employees referred to download the app by their organisation
- Used by coaches to support clients

Participants could use the app:

- As a standalone tracking tool
- As part of a wellbeing challenge
- As part of a coaching course
- As part of an event/fundraiser

Commitment statement

The EU General Data Protection Regulation (GDPR) is the most significant piece of European privacy legislation in the last twenty years. It replaces the 1995 EU Data Protection Directive (European Directive 95/46/EC), strengthening the rights that EU individuals have over their data, and creating a uniform data protection law across Europe.

We will comply with applicable GDPR regulations as a data processor when they take effect on 25th May 2018. Working in conjunction with our clients, we will explore opportunities within our services offerings to assist our customers to meet their GDPR obligations

Associated documents

1. Privacy document
2. Consent statements
3. Supporting documentation from Armor data security

1.0 GDPR COMPLIANCE OVERVIEW

GDPR requirements

- **Notification of data breaches –** When we are aware of a data breach of personal or sensitive personal data, we understand that we have a 72-hour window to notify the relevant supervisory authority of the breach. Additionally, we must individually notify data subjects of any breach that presents a high risk to their individual rights and freedoms.
    - Responsibility – Wellbeing4business Ltd
    - Security and rapid response – Nudge and Armor

- **Ability to demonstrate compliance** – This document outlines our understanding of the security requirements prescribed directly or indirectly by the regulating party to demonstrate compliance. We have aligned our data with the secure cloud controls that meet these specific requirements.
    - Refer to this document
    - See privacy policy
    - See consent statements
    - See Armor - https://www.armor.com/gdpr/
    - See Nudge - https://nudgecoach.com/hipaa-compliance

- **Right to data portability** – We have ensured that participants know that they have the right to data portability, which means they can request the personal data they have supplied. Data will be delivered in "a structured, commonly used and machine-readable format" in order to transfer aforementioned personal data to another data controller.
    - Refer to consent statements

- **Right of access** – Participants are informed that they have the right to know if and when their data is transferred to a third country or an international organization. Safeguards are required to ensure ongoing protection of the data after transfer.
    - Refer to this document
    - See privacy policy
    - See consent statements

- **Right to erasure (right to be forgotten**) - Participants are informed that they have the right to request the erasure of personal data held by a data controller, subject to certain conditions. We are clear about processing data, the appropriate legal basis, and when required, we have a technological ability to erase all affected data promptly.
    - Refer to this document
    - See privacy policy
    - See consent statement

- **Security of processing** – We have implemented technical and organizational measures to ensure an appropriate level of security is in place for processing activities. These activities include, but are not limited to, pseudonymization, encryption and regular testing of organizational and technical measures.
    - Refer to this document
    - See privacy policy
    - See consent statements
- **Transfers of personal data to third countries or international organizations** - The GDPR outlines specific requirements governing when and where personal data can be transferred to third countries or international organization
    - Refer to this document
    - See privacy policy
    - See consent statements

2.0 COMPLIANCE INFORMATION

The following information outlines the steps taken and procedures in complying with GDPR.

2.0.1 – LEGITIMATE INTERESTS

- We explain clearly how or why we need an individual's personal data when we collect it throughout the app download and coaches forward a consent statement to all participant opting for coaching
- We have a Privacy Policy that puts the most important information upfront and then there is a more detailed privacy policy underneath it
- Individuals are well informed of what we plan to do with their data when we collect it through
- We clearly state that we do not use data for marketing to third parties
- We collect the minimum data necessary (Individuals can choose what data to enter and although we collect a minimum of name and email this can be fictitious if required
- We delete records after use. If an individual asks us to delete their data from our systems, we delete their data from our systems completely and with reasonable expediency. The individual can delete the app at any time from their phone

Refer to: our Privacy policy, consent statement and terms and conditions

2.0.2 – OBTAINING AND INFORMING ON CONSENT

Asking for consent

- We ask people to positively opt-in – individuals are **invited** to download the app and **choose** to opt for coaching
- We do not use pre-ticked boxes or any other type of consent by default
- We use clear, plain easy to understand language at each process
- We explain why we want the data and what we're going to do with it
- We name our organisation and third parties who can access the data
- We inform individuals they can withdraw their consent
- We inform the individual they can refuse to consent to options such as coaching
- We don't make consent a precondition of our service
- We are clear that we do not provide services to children

Recording consent

- We keep a record of when individuals refuse consent or wish to delete records
- We keep a record of exactly what they were told at the time

Managing consent

- We regularly review consent to make sure that the relationship, the processing and the purposes have not changed since consent was given
- We have the means to refresh consent at appropriate intervals, including any parental consents
- We make it easy for individuals to withdraw their consent at any time, and show them how to do so
- When consent is withdrawn, we act as soon as we can
- We don't penalise individuals who want to withdraw their consent

Refer to: our Privacy policy, consent statement and terms and conditions

2.0.3 – INFORMATION PROVISIONS

When collecting personal data we make sure individuals are aware of the following:

- The identity and contact details of our organisation
- Contact details of the data protection responsible person are clear on the WELL121 website
- The consent or legitimate interests necessary for data processing and why
- If your organisation uses legitimate interests legal grounds to contact individuals – individuals can chose to allow notifications and opt into coaching.
- Other countries outside the EU the data may be processed
- Tell individuals about their right to have their personal data deleted and to object to data processing in the future
- The right to complain to the national data protection authority

2.0.4 – THIRD PARTY DATA

- We do not supply data to any third parties for business or marketing reasons
- We clearly state this in our Privacy policy

Third Party Services

- We may use a variety of services offered by third parties to help maintain and improve our Website, to help us understand the use of our Website and Services, or simply to provide the Services.
- These services may store both personally identifiable information about you which we collect and the information sent by your browser as part of a web page request, such as cookies or your IP address.
- If any third parties are given access to your personally identifiable information, we will limit the use of such personally identifiable information only to provide the services to us which we have requested

Coaching Services

- Wellbeing4business will use both employed and subcontracted coaches
- All coaches are required to have professional qualifications in their area of expertise and valid certification
- All coaches will be fully trained on the coaching system
- All coaches will be named per and participants made aware when coaching
- All coaches will carry valid insurances
- All coaches will forward a consent statement explaining how and why we share participant data. If participants accept an invitation from a Well 1-2-1 Coach, the Coach will be able access to all data and information that exists under the account. The Coach will also be able to send private messages to through the chat function. The Coach has agreed to keep your data and information confidential and not use it for any purpose other than to provide you individualized advice and services, but we cannot provide any assurances that any Well 1-2-1 Coach will in fact do so. We are not required to litigate or otherwise pursue any wrongful disclosure of data and information. To the extent that any data or information contains protected health information, consenting participants expressly consent to the disclosure of such protected health information when you accept an invitation from a Coach.
- All participants can turn off coaching at any time and ask for information to be deleted.
- All complaints will be managed through our formal complaints process

Coach licences

- Coaches and healthcare providers may lease our platform to use with their clients
- All licences will clearly state that the management f client data is under the governance of that coach/provider and all contacts must adhere to the terms and conditions of licence.
- All licencees can only see their own data**.**

2.0.5 - PROFILING

Profiling means evaluating personal data so you can review individual or group data.

- We provide data results on our leader boards clearly for all to see
- We provide data reports to organisations using anonymous data and inform people that any group reports will not only be completed on 10+ participants and will respect medical and client confidentiality.
- Marketing communications for all services include detail on use of data
- We tell people how and why we profile personal data but give people the chance to opt-out
- We explain how we profile an individual's personal data in your privacy notice/policy

2.0.6 – LEGACY DATA

- We will not continue contacting individuals after the event (challenges, coaching) has finished.
- All data is deleted following an event completion if required by an organisation or individual.
- If an individual wishes to delete their records; they can delete the app off their device and inform us on info@wellbeing4business.co.uk and we will o so expediently.

2.0. 7 – DATA STORAGE AND SECURITY

We use third party vendors and hosting partners to provide the necessary hardware, software, networking, storage, and related technology required to run WELL121. We do not transfer ownership of any code, databases, Website rights or data to any third party vendors or hosting partners.

https://www.armor.com/how-we-work/

Creating a HIPAA-compliant digital coaching platform begins with where all the data lives, and for us, that begins with our first key partner in HIPAA-compliance and security, and that's leading ***cloud-based*** secure hosting provider, Armor.

GDPR compliance - Armor.

- Certified Compliant: Security that delivers. And, we have the certifications to prove it: PCI DSS, HITRUST, ISO 27001, SSAE 16 SOC II and Privacy Shield Framework.
- Built for Cloud Compliance: Our managed cloud security solutions were built to address risk-based compliance standards like GDPR and HIPAA.
- GDPR Compliance Support: Our security team – from our analysts up to our CISO – provide 24/7/365 customized, hands-on support to help you overcome any compliance challenge

Armor built-in security capabilities address critical areas of GDPR compliance:

Network

- Intrusion Detection: detects malicious traffic that could result in data breaches
- Vulnerability Scanning: reduces attack surface by identifying improper configurations and missing patches/updates
- IP Reputation Management: effective first-line-of-defense in blocking IP addresses associated with threat actors
- Web Application Firewall: provide effective detection and blocking of traffic associated with malicious application behavior such as cross-site scripts, SQL injection.

Server

- File Integrity Monitoring: monitors unauthorized changes to critical files

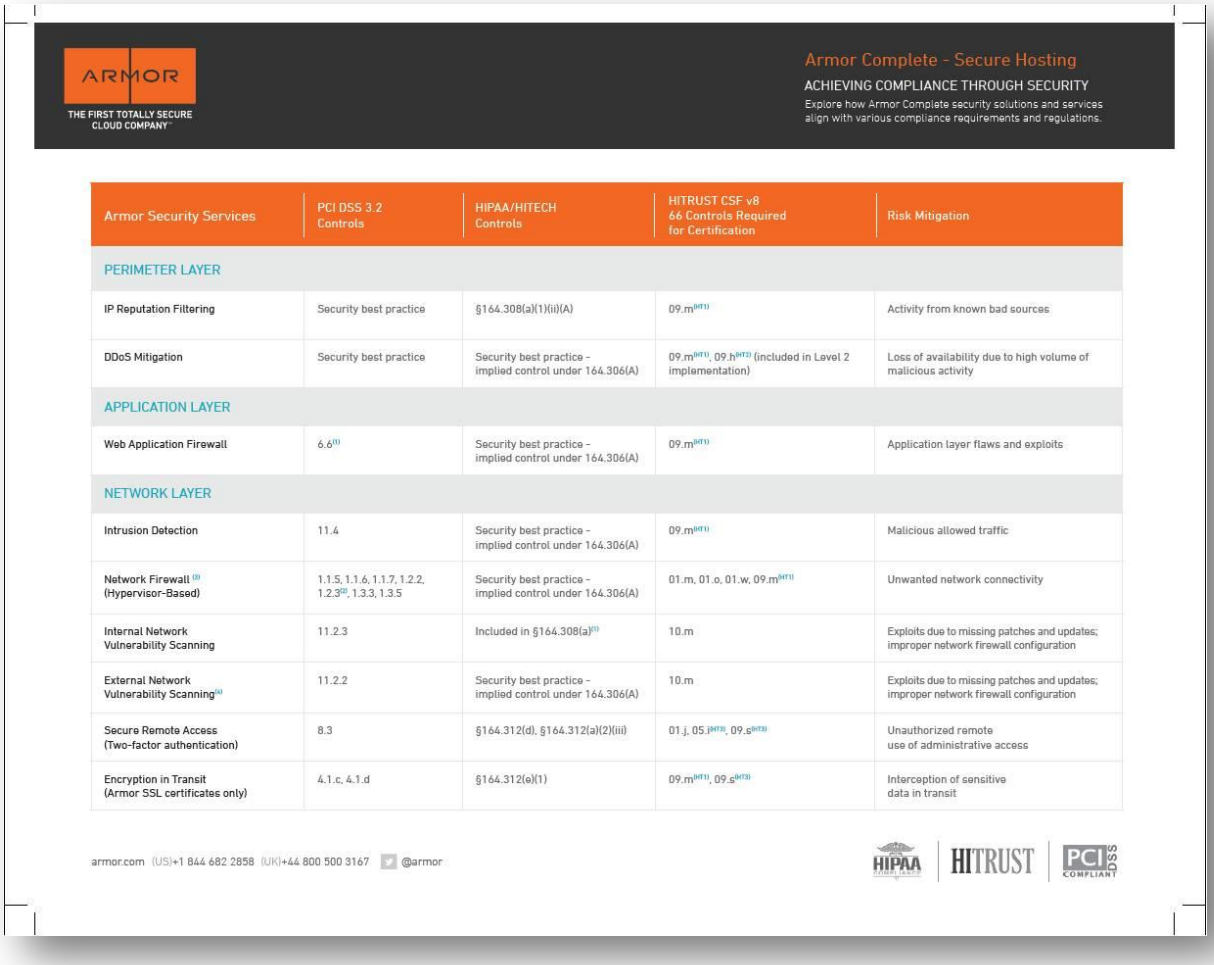
- O/S Patching: addresses O/S vulnerabilities
- Malware Protection: protects systems from viruses and malware
- O/S Log Management: records history of important O/S events for response and forensics investigations

Administration

- Security Dashboard: facilitates documentation of security posture and incident communication
- Incident Response: provides quick and prioritized response to incidents

Compliance Matrix Armour

See https://www.armor.com/gdpr/



ARMOR
THE FIRST TOTALLY SECURE CLOUD COMPANY

Armor Complete - Secure Hosting
ACHIEVING COMPLIANCE THROUGH SECURITY
Explore how Armor Complete security solutions and services align with various compliance requirements and regulations.

Armor Security Services	PCI DSS 3.2 Controls	HIPAA/HITECH Controls	HITRUST CSF v8 66 Controls Required for Certification	Risk Mitigation
PERIMETER LAYER				
IP Reputation Filtering	Security best practice	§164.308(a)(1)(ii)(A)	09.m[HT1]	Activity from known bad sources
DDoS Mitigation	Security best practice	Security best practice - implied control under 164.306(A)	09.m[HT1], 09.h[HT2] (included in Level 2 implementation)	Loss of availability due to high volume of malicious activity
APPLICATION LAYER				
Web Application Firewall	6.6[1]	Security best practice - implied control under 164.306(A)	09.m[HT1]	Application layer flaws and exploits
NETWORK LAYER				
Intrusion Detection	11.4	Security best practice - implied control under 164.306(A)	09.m[HT1]	Malicious allowed traffic
Network Firewall [3] (Hypervisor-Based)	1.1.5, 1.1.6, 1.1.7, 1.2.2, 1.2.3[2], 1.3.3, 1.3.5	Security best practice - implied control under 164.306(A)	01.m, 01.o, 01.w, 09.m[HT1]	Unwanted network connectivity
Internal Network Vulnerability Scanning	11.2.3	Included in §164.308(a)[1]	10.m	Exploits due to missing patches and updates; improper network firewall configuration
External Network Vulnerability Scanning[4]	11.2.2	Security best practice - implied control under 164.306(A)	10.m	Exploits due to missing patches and updates; improper network firewall configuration
Secure Remote Access (Two-factor authentication)	8.3	§164.312(d), §164.312(a)(2)(iii)	01.j, 05.j[HT3], 09.s[HT3]	Unauthorized remote use of administrative access
Encryption in Transit (Armor SSL certificates only)	4.1.c, 4.1.d	§164.312(e)(1)	09.m[HT1], 09.s[HT3]	Interception of sensitive data in transit

armor.com (US)+1 844 682 2858 (UK)+44 800 500 3167 @armor

HIPAA | HITRUST | PCI DSS COMPLIANT

2.0.8 FURTHER INFORMATION

Contact us on 01257453645 or email info@wellbeing4business.co.uk