BPF Fitness Hub Tetbury GDPR compliance, policies and methodologies

1. We have a **data protection compliance folder** on the BPF Fitness Hub file system containing GDPR documentation and we keep a record of **consents to hold data** via Membership Forms, Direct Debit Mandates and Physical Activity Readiness Questionnaires (PARQ) – our acquired customer data consists of customer names and business identities (where appropriate,) and email and postal address detail, telephone details, D.O.B and bank details.
2. We **note** meetings on GDPR, and decisions made on GDPR, through our usual meeting and minutes process at BPF Fitness Hub.
3. The Advertiser **data protection officer** Andrea Herbert, Director BPF Fitness Hub.
4. Our data is **Mapped** into three categories:
5. A) Memberships with active "Accounts"
   B) Archived, non-active / frozen memberships.
6. C) Cancelled Memberships.
   The purpose of these categories is firstly to database, bill, track and occasionally incentivise members, secondly (category B,) to retain membership material for potential re-use by customers who are no longer running "active" memberships.
7. We assert the **lawful basis** for both these categories, chiefly through (although not restricted to,) items a, b and c of article 6 of the GDPR. The specific terms from the act state:

   (a) the data subject has given consent to the processing of their personal data for one or more specific purposes;
   (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
   (c) processing is necessary for compliance with a legal obligation to which the controller is subject.

8. We practice a policy of **refreshed consent** where necessary.
9. We have a policy to handle any **data subject access requests.**
10. We have a policy to handle any **data erasure or corrections requests.**
11. We are prepared to document **non-compliance issues** and risk mitigation.
12. We have a **password policy** for users of the Accounts system, web site and collection and preparation equipment used for BPF Fitness Hub.
13. We contacted our database of current and previous customers to ask them to **opt in** to our data retention.
14. We have a **retention schedule** for data, in respect of both active customer data and archived membership information. We minimise the data we hold. Accounts data is held for six years, in keeping with prudent practice. "Front End" contact information is retained for two years or length of membership contract if longer, to preserve contract details and allow contact with customers *with their permission.* Cancelled information is retained for seven years unless expressly asked to be permanently deleted by the client.
15. Our staff and volunteers all understand **what constitutes personal data.**

16. Our staff and volunteers can **identify a breach** and how to avoid email scams, phishing processes and so on.
17. We have a **breach response policy.**
18. We hold a **data breach log** to record events.
19. Our website has **HTTPS** security, since it is for information and payment processing..
20. Our office **computers are encrypted** using “security by design.”
21. We review the **physical security** of our data regularly; disks, paper filing systems and all other retention is “behind lock and key.”
22. We hold an **asset register** of the serial numbers of our computers.
23. We have a register of individuals with **access to the data on each device.**
24. We securely **lock away any data.**
25. We have a **privacy policy – this document -** (which includes identity of the data protection officer, the purpose of the processing and the legal basis, the legitimate interest, any recipient or categories of recipients of the personal data, the right to withdraw consent at any time, and the data retention period.)
26. We have an **ongoing consultation procedure** to re-visit our processes, both technical and legal, in case of a new requirement, to take simple further steps before we are fully compliant, or to retain compliance.
27. BPF Fitness Hub employs a proprietary Accounts system via Quickbooks - a modern cloud-based system with built-in scheduled backup and restoration processes: Quickbooks Privacy Policy and a database system via E Z Facility who have their own built in security, backup and restoration processes: E Z Facility Privacy Policy Security and data protection is inherent in the design.
28. Card payments are taken via SumUp whose GDPR and Privacy Policies can be viewed here: SumUp GDPR
29. . No unprotected devices are permitted to access data.
30. Please contact the Advertiser Data Protection Officer - the editor - if you would like more specific details about any of the procedures or policies set out in this document.