Data Protection key points under GDPR

The General Data Protection Regulation (GDPR) will take effect in the UK on 25 May 2018. It replaces the existing law on data protection (the Data Protection Act 1998) and gives individuals more rights and protection in how their personal data is used by organisations. The Polish Catholic Mission must comply with its requirements, just like any other charity or organisation.

The law is complex, but there are a number of underlying principles, including that personal data:

1. Will be processed lawfully, fairly and transparently.
2. Is only used for a specific processing purpose that the data subject has been made aware of and no other, without further consent.
3. Collected on a data subject should be “adequate, relevant and limited”. i.e. only the minimum amount of data should be kept for specific processing.
4. Must be “accurate and where necessary kept up to date”
5. Should not be stored for longer than is necessary, and that storage is safe and secure.

Personal data is information relating to a living individual, who can be identified directly from that data or indirectly by reference to other data held.
Processing is anything done with/to personal data, including storing it.
The **data subject** is the person about whom personal data are processed.
The **data controller** is the person or organisation who determines the how and what of data processing.
Special category data is data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation. Special rules apply including rules around no disclosure to third parties without consent.

Key points

1. There are several legal bases for processing data, of which **consent** is one. Others include **legal obligation** (e.g. processing Gift Aid), **contract** (letting out the premises), or **legitimate interest** (members lists). For each area of processing you will need to be clear on your legal basis for carrying out that processing.

Podstawowa informacja nt. ochrony danych w ramach GDPR

Ogólne rozporządzenie o ochronie danych (GDRP General Data Protection Regulation) wejdzie w życie w Wielkiej Brytanii w dniu 25 maja 2018 r. Zastąpi ono istniejącą ustawę o ochronie danych (ustawa o ochronie danych z 1998 r.) i zapewni osobom prywatnym więcej praw i ochronę w zakresie wykorzystywania ich danych osobowych przez organizacje. Polska Misja Katolicka musi spełniać te wymagania, tak jak każda inna organizacja, czy organizacja charytatywna.

Prawo jest skomplikowane, ale istnieje kilka podstawowych zasad m.in., że dane osobowe:

1. Będą przetwarzane zgodnie z prawem, uczciwie i przejrzyście.
2. Będą wykorzystywane wyłącznie do określonego celu przetwarzania, o którym poinformowano osobę, której te dane dotyczą, a nie do żadnego innego celu, bez dodatkowej zgody.
3. Zebrane dane na temat osoby, której dane dotyczą, powinny być "odpowiednie, istotne i ograniczone". To znaczy, że tylko minimalna ilość danych powinna być przechowywana dla konkretnego przetwarzania.
4. Muszą być "dokładne i w razie potrzeby aktualizowane".
5. Nie należy przechowywać dłużej niż to konieczne, a że miejsce przechowania jest zabezpieczone.

Dane osobowe to informacje dotyczące żyjącej osoby, które można zidentyfikować bezpośrednio z tych danych lub pośrednio, poprzez odniesienie do innych posiadanych danych.
Przetwarzanie to proces, co robi się z danymi osobowymi włącznie z ich przechowywaniem.
Podmiotem danych jest osoba, której dotyczą przetwarzane dane osobowe.
Administratorem danych jest osoba lub organizacja, która określa sposób i granice przetwarzania danych.
Dane kategorii specjalnej to dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne lub przynależność do związków zawodowych, przetwarzanie danych genetycznych, dane biometryczne w celu jednoznacznej identyfikacji osoby fizycznej, dane dotyczące zdrowia lub dane dotyczące życia seksualnego osoby fizycznej lub orientacji seksualnej. Obowiązują specjalne zasady, w tym zasady dotyczące nie ujawnienia danych osobom trzecim bez zgody podmiotu danych.

Główne Punkty

1. Istnieje kilka podstaw prawnych przetwarzania danych: **zgoda, prawne zobowiązanie** (np. Przetwarzanie danych Gift Aid), **umowy** (np. wynajmowanie pomieszczenia) lub **uzasadnione zainteresowanie** (np. spis członków). W przypadku każdej dziedziny przetwarzania konieczne jest podanie jasnych podstaw prawnych do przeprowadzenia danych.

2. You may need to have consent from people for some data processing; e.g. some email communications, or whether data is share with members such as in a church directory. This will need to be clear and unambiguous – some form of positive action to “opt-in”. You must ensure you have this consent before processing.
3. Data subjects have a number of rights, including that of knowing how data is used by the data controller, of knowing what data is held about them, of correcting any errors and generally the right ‘to be forgotten’. Provision will need to be made for people to exercise these rights, including developing a Privacy Notice.
4. The GDPR introduces a stronger requirement on accountability for data controllers. This means that you must be able to show that you are complying with the principles by providing evidence. For example, where you process on the basis of consent, you should store these consents.
5. Where data “reveals religious belief” it becomes special category data – which requires additional care with regard to processing. A second legal basis is required for processing special category data, but the GDPR allows religious (amongst others) not-for-profit bodies to process such data without specific consent as long as it relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent.

Carry out a data audit: review what data you hold, how you store it, and what basis you have for processing it.

Here are some questions to help you carry out your audit:

- What kind of data is being collected and stored, where and why?
- Which different church groups might store their own data? Make sure you cover them.
- How is the data used (i.e. processed) both internally and externally?
- How long is the data retained?
- Who has access to the data both inside and outside of the LPCM?
- What procedures and controls are in place to keep data safe?

It’s likely that your audit will identify some areas where your current data systems or processes are not compliant with the GDPR, and so the final column enables you to identify action that might be required. In some cases, you might decide that data is no longer needed to be held and processed, in other cases, it might be changes to how you store the data or who has access to it.

2. Może zaistnieć potrzeba uzyskania zgody od ludzi na przetwarzanie danych; na przykład niektóre wiadomości e-mailowe lub udostępnianie innym członkom np. w katalogu kościoła. Należy to robić jasno i jednoznacznie w formie pozytywnego działania, jak na przykład "opt-in". Trzeba upewnić się, że jest taka zgoda przed przetwarzaniem danych.
3. Podmioty danych mają wiele praw, w tym możliwość wiedzy o tym, w jaki sposób dane są wykorzystywane przez administratora danych, o tym, jakie dane są przechowywane na ich temat, o poprawieniu wszelkich błędów i ogólnie o prawie do „bycia zapomnianym”. Należy wprowadzić przepisy umożliwiające ludziom korzystanie z tych praw, w tym opracowywanie informacji na temat ochrony prywatności.
4. GDPR wprowadza wymóg większej odpowiedzialności administratorów danych. Oznacza to, że musimy być w stanie wykazać, że przestrzegamy zasady prawne, dostarczając dowodów. Na przykład, jeśli przetwarzamy dane na podstawie zgody, powinniśmy przechowywać dokument wyrażający zgodę.
5. Jeżeli dane "ujawniają przekonania religijne", stają się one danymi kategorii specjalnej - co wymaga dodatkowej czujności w odniesieniu do przetwarzania. Druga podstawa prawna jest wymagana do przetwarzania danych o specjalnej kategorii, ale GDPR pozwala religijnym organizacjom „non-profit” (między innymi) na przetwarzanie takich danych bez wyraźnej zgody, o ile odnosi się tylko do członków lub byłych członków (lub tych, którzy mają regularny kontakt z nim w związku z tymi celami) i pod warunkiem, że nie ujawnia się stronom trzecim bez zgody.

Przeprowadzić audyt danych: Sprawdź, jakie dane przechowujesz, jak je przechowujesz, i jakie masz podstawy do ich przetwarzania.

Oto kilka pytań, które można zadać, a które pomogą przeprowadzić audyt:

- Jakie rodzaje danych są gromadzone i przechowywane, gdzie i dlaczego?
- Jakie różne grupy kościelne mogą przechowywać własne dane? Upewnij się, że je uwzględniasz. (np. schola, grupa różańcowa)
- W jaki sposób dane są wykorzystywane (tzn. przetwarzane) zarówno wewnętrznie, jak i zewnętrznie?
- Jak długo przechowywane są dane?
- Kto ma dostęp do danych zarówno w lokalnej Polskiej Misji Katolickiej, jak i poza nią?
- Jakie procedury i kontrole są stosowane, aby zapewnić bezpieczeństwo danych?

Jest możliwe, że w wyniku audytu okaże się, że obecne systemy lub procesy danych nie są zgodne z GDPR, a więc końcowa kolumna umożliwia określenie działań, które należy wykonać. W niektórych przypadkach można zdecydować, że dane nie są już potrzebne do przechowywania i przetwarzania, w innych przypadkach mogą to być zmiany sposobu przechowywania danych.