UPDATA

110010000110
001010011110
1001001100110
0011011110001
110010000110
001010011110

September 2019

This bulletin is intended for Parish Secretaries, administrators, rota coordinators and newsletter editors.

15 months after the coming into force of the GDPR, I have accumulated a number of Good Practice tips and recommendations from national meetings of Data Protection Officers working in Catholic Dioceses, and I hope this will be a useful "updater" format in which to share them with you

Brin Dunsire
Data Protection Manager

DATA PROTECTION

Sick lists

I'm putting this first because I have been persuaded to **modify the advice** I have been handing-out on this, especially in the **Guide for Parish Volunteers** which I issued in July 2018 and have distributed widely since.

We are talking about the lists of names of parishioners who are unwell, which are published in parish bulletins/newsletters -and because these are often reproduced on the parish website, they are seen online and are potentially visible to anyone in the world, including crooks and fraudsters.

I have hitherto taken the view that the risk of any harm arising from this practice, which serves a much-valued pastoral purpose, is very slight, and that we should not interfere with it in the name of Data Protection. After all, the people named would, more often than not, be quite happy at the thought that their parish community was praying for them by name.

However, the fact is that we are disclosing, without the subject's specific consent, the names of parishioners in association with a Catholic parish in a particular place, thus giving out information about their religious affiliation, and this in itself is "special category data" ; we then double up on this by disclosing the sensitive fact that they are in poor health. It is the firm advice of our insurers' legal department that while this might be acceptable in the printed parish bulletin, seen only by the Mass-going community and a few extra people who may have the bulletin taken home to them, the online publication of these names is not something we can defend or justify.

We still do not want to prohibit the practice; but **we must now advise that a different version of the parish bulletin should be prepared for online publication,** omitting these lists of names. If there is strong demand for a digital version of the full bulletin, maybe from those who cannot get to Mass and are not having a paper version brought to them, maybe a full version could be distributed by email or a password issued to gain access to a full version published in a restricted section of the parish website. We

only have to go to these lengths because it will rarely be practicable to obtain the specific consent of every person being named ; frequently the request for a name to be included is made by a close family member, or even a friend

Speaking out names in Bidding Prayers or when announcing the Mass intentions is fine, as is listing the recently-deceased, for Data Protection does not apply to the dead.

CCTV in parishes and their car parks

Increasingly, churches are installing some form of CCTV, and while this has advantages in the discouragement (and detection) of crime and anti-social behaviour, we have to be aware that it represents a constant invasion of privacy for our parishioners and visitors, and amounts to "processing " of personal data - people's images and appearances *are* their personal data, as much as their names and addresses. Therefore, we have to warn them that this data is being collected, explain the purpose of the collection, and give them information about their rights over it . This is normally done by sizeable notices placed at the entrances to car parks and buildings, and the companies that install CCTV systems for you will usually offer to do this as part of their services, but they do not always get the wording right. Our insurers have produced substantial guidance about CCTV systems in parishes, including a specimen notice, and you should ensure that this is complied with, either by replacing existing notices or bringing it to the attention of any contractor installing a new system. The document is available as a download from the diocesan website at www.northamptondiocese.org/data.

One aspect of CCTV surveillance in parish car parks which has already come up and is likely to recur, is the following scenario:

A car-park user causes damage to another car and drives away, either not realising what they have done or choosing not to report the accident or leave a note on the damaged car. The owner of the damaged car storms in and demands to see your CCTV footage of the car park, so that they can identify the number plate of the offending car and thereby track down the driver – or, you receive a formal request from the insurers of the damaged car, or from solicitors, to provide the registration number of the offending car, or an excerpt of the CCTV footage. The ICO has ruled that a car registration plate is personal data, because from it, an individual can be traced and identified, even though this capacity is not easily available to the general public. Strictly, therefore, you should not release the registration number or the footage without the consent of the offending driver, which in the nature of things is unlikely to be forthcoming. You may not even know who the offending driver was, if you cannot identify a known individual from the footage. What are you obliged to do?

Certainly, even if you are able to identify the offender immediately from your footage, you must not show this to the angry "victim" or give out the name of the offender. You can and should explain that you *will* provide the information on receipt of a formal request from the claimant's insurers or solicitors. That request must identify their client, state that the information is required for the purposes of legal proceedings, and identify with as much detail as possible the car alleged to have caused the damage, and the one alleged to have suffered damage

If all they are after is a registration number, you can give them a still photo which makes this clear, but if they are asking for a section of moving footage, you will probably have to engage a specialist firm to edit your video footage down to a small relevant section, including obscuring the number plates of nearby cars. This could prove expensive ! If you do know who caused the damage, you can explain this in seeking to persuade them that they *should* consent to you disclosing their name to the insurers/lawyers, since if they do not, the parish will at some point be subjected to a Court Order compelling disclosure of the information, and this will increase the costs payable by the offending driver. Also, one hopes they would not wish to expose their parish to unnecessary costs and a lot of work arising from their moment of carelessness, and would agree to providing information and maybe even admitting fault.

Your CCTV notices should, if there is room, include a notification that images recorded may be provided to the police, to insurance companies, and/or to third parties as required by law. Clearly, if the police ask for your CCTV footage in connection with the investigation of a crime, you must provide it.

There is more to say about the slightly different issue of "live streaming" of televised masses and parish events, but as that is not yet widespread we will leave it for another time

Providing baptismal certificates

As I explained on my roadshows last year, one of the occasions where Catholic parishes frequently hand out red-hot information about parishioners to unknown, and possibly malicious, enquirers, is in the ready provision of baptism and confirmation certificates. Apart from the fact that they disclose quite a lot of sensitive personal data, they are very useful documents for fraudsters, as they are sometimes acceptable as proof of identity, helping to procure the issue of fake passports and other identity- fraud documents. When faced with a request – often urgent, and backed up with a plausible story – to provide a baptismal certificate, parish secretaries need to satisfy themselves that the enquirer is entitled to the information , and is actually who they say they are.

Consider the following perfectly plausible phone call:

“"Hello, my name is Joe Smith. I was christened in your church 30 years ago and I'm getting married next week. I've only just found out that I am supposed to provide a baptism certificate to the priest who is marrying us. Can you e-mail me a scan of it as quickly as possible, please?"

Photo by Paula Lavalle on Unsplash

Assuming you don't know who Joe Smith is, and don't recognise his voice, your first question should be:

"Are you local? Can you call in with some ID like a driving licence or passport, and then we'll give you the certificate straight away" - Because if it is the genuine Joe Smith, he is entitled to be given this information about himself, and you do not need that at that stage to insist that the request must come from the church where he is getting married

However, the response is likely to be:

"No, I'm abroad/a long way away, and I can't get to you. But I need this thing urgently, because if I can't get it to the priest by Friday, the wedding will have to be cancelled and we'll lose thousands"

Your next line is "okay, I'll go and see if we've got the information you want, ring me back in 10 minutes"

You dig out the baptismal register from the 1980s and you do indeed find a Joseph Smith. When he rings back, you ask him for his full name, and the names of his parents and godparents. If he can immediately give this information, it is likely that he is indeed the right person, though we can make allowances for the fact that some people have never been told who their godparents were. Having satisfied yourself on his identity, this is the point to ask for the name of the priest and parish who want the information and to promise that you will send a scan of the certificate directly to them, straight away. Before doing so, you will look up the parish on the Internet and make sure that it exists, and has a priest of the name given

If you are in any way suspicious about the enquirer, you should tell him that he must get the priest to contact you directly and make a request for the certificate. If this comes through, you would check out the parish and the priest, and you can then send them what you are requesting.

If there is the least uncertainty in your mind about complying with the requests, but you basically want to be helpful, you should make a note in your "Data Protection" notebook that I have recommended all secretaries should keep, recording the circumstances of the request, what steps you took to verify his identity, and why you have decided it was okay to take a slight risk. If we make a mistaken judgement, and some harm comes from it which is being investigated years later, we will have covered ourselves by proving that

we took what steps we could and were not being careless. And don't be pressurised or bullied into taking an undue risk – you are perfectly entitled to hide behind Data Protection law, and it is not your fault that the enquirer has left it far too late !

It is also perfectly likely that the initial phone call may come from Joe Smith's mother, with a sob story that her son is useless at organising anything, and has asked for her help – or that he is on a mining job in Alaska, and has no access to the Internet and only an occasional phone signal. You *cannot* hand out his certificate to her, even if she can give the correct details to match the register - in these circumstances, you *must* have the request from the priest who needs the information

Data breaches

Here are some examples of "data breaches " reported to their Dioceses by conscientious parishes (but not necessarily passed upwards to the Information Commissioner ; it is not clear where the line is drawn between identifying a risky practice / sloppy procedure, and labelling something as a "data breach". However, if in doubt, let me know about it, as it is my job to decide whether it is serious enough to justify being reported further.)

- A list of names of children about to make their First Holy Communion left lying around on open view at a primary school. (Printing them in a Service booklet will have been consented-to)
- The uploading of a Rota containing personal data (phone numbers and e-mails) to a parish website
- An envelope containing sensitive personal data (which could mean religious affiliation, health information, sexuality information etc, or maybe a communication to or from a safeguarding office with case details) being posted by ordinary post rather than Guaranteed Special Delivery or "Signed For " post. It is arguable that there is no greater level of information security by paying the higher delivery charges, as opening or delaying the post is illegal at all levels, but if there is any suggestion that you have allowed sensitive material to go astray, having proof that it was received intact at the destination address may be important
- Emails being sent to the wrong person - a moment's inattention, combined with the auto-fill feature of many email systems, can result in a disastrous misdirection of a sensitive email, leading to a complaint by anyone harmed.
- Emails being sent to a large block of addresses without using the BCc feature - the IICSA Child Protection Enquiry was fined £200,000 for a careless error of this nature, some of the identities of the addressees which were revealed by their email addresses being extremely sensitive
- A priest's iPad , which he was using to make end-of-Mass announcements, was stolen from the lectern when he left it unattended for a couple of minutes ; fortunately he knew how to disable it remotely, and took immediate action - would you be able to do this if your smartphone or tablet was stolen ?

Sign-up lists

I still take the view that these lists, familiar from parish notice-boards where people sign-up for anything from a parish barbecue to a twelve-week course, are low-risk, as few crooks would go to the trouble of photographing and re-typing a few phone numbers and e-mails ; but my colleagues assure me that some people *have* reported unwelcome calls to their new mobiles within days of putting the number on a parish list, so it is safest to add a clause like this to the foot of any such notice:

Data Protection - Your personal details given above will be stored and used by the Parish only for the purposes of running and administering the [Jubilee dinner] [Carol concert] . They will not otherwise be disclosed outside the parish. Details of how we process your data, and your rights, are on the full Privacy Notice which is on the noticeboard and/or may be seen in the Parish Office and/or on the (Diocesan) website. If you are concerned about your details being misused, please find another way of giving them securely to the event organiser.