GDPR webinar – supporting you on your voyage to compliance
Q&As

We had a great response to our GDPR webinar on Thursday 8 March 2018, please find below a summary of the questions we received during the webinar:

Consent

Q: If you already have obtained consent for marketing, positive or otherwise, do you need to seek consent again for GDPR? In my opinion, if you do, this would not be productive.

A: Any consent that you have must meet the requirements of the GDPR in order to be considered valid. If it does not meet these requirements you should consider whether you need to re-obtain consent or use another legal basis of processing.

Q: If we receive personal data via a corporate client, who gets the consent? For example, driving licenses within a motor fleet client?

A: Consent needs to be obtained at the point that the personal data is collected, if that is your legal basis of processing.

Q: We call all lapsed cases when the policy comes up for renewal in the year after the policy lapsed to see if the client would like a quotation. Will we need consent to do this from the client?

A: Not necessarily, you should review your legal basis of processing options to determine the best basis on which to carry out this activity.

Q: Do we need to contact all policy holders prior to renewal invitation to ask their consent to use existing data to process renewal?

A: Not necessarily, you should review your legal basis of processing options to determine the best basis on which to carry out this activity.

Q: How often does consent need renewing?

A: The ICO and the Article 29 Working Party have issued consent guidance, which includes consent renewal.

Q: Does cross selling require consent? For example, marketing cyber cover to commercial clients?

A: Not necessarily, you should review your legal basis of processing options to determine the best basis on which to carry out this activity. You should also review the Privacy and Electronic Communications Regulations in relation to marketing activities.

Fair Processing Notice (FPN)

Q: As an insurance broker, where should you publish your privacy notices?

A: The ICO has provided guidance on privacy notice and the transparency requirements, including how these should be displayed to individuals.

Q: Am I correct in thinking that you cannot put your written Privacy Notice in your clients Terms of Business and Status Disclosure.

A: The ICO has provided guidance on privacy notice and the transparency requirements, including what information should be provided and where these should be displayed to individuals.

GDPR webinar – supporting you on your voyage to compliance

Q&As

Retaining information

Q: What should we do with e-mail addresses on a prospect database where they have made an enquiry in the past? Do we have to get consent for storage and contact for quotation purposes in the future?

A: You should look at your legal basis of processing, this does not necessarily need to be consent.

Q: With regards to the obligation to securely delete/dispose of personal data when no longer needed - what about regulatory guidance to keep records under ICOBS 2.4? For brokers who could face professional indemnity claims years after the policy has lapsed, surely we should retain our records to provide evidence in the event of a dispute?

A: Personal data should not be retained for longer than is necessary under GDPR, which is an existing requirement under the Data Protection Act. You will need to determine what "necessary" means for your business. We recommend visiting the ICO's website for further information.

Q: If we process medical information by way of receiving statements of health from clients, how long can we keep it? Only for the time of the production policy? How should this be destroyed as it will be on the server so what are the implications for that?

A: Personal data should not be retained for longer than is necessary under GDPR, as it is today under the Data Protection Act. What is necessary is up to you to determine. Personal data should be securely deleted at the end of the retention period.

Q: What is Hiscox's information retention policy timescales? Do customers need to be advised how long information is held specifically?

A: Hiscox have updated our own retention policy and detailed schedules. The exact retention times vary across different types of personal data across the business.
The requirements for privacy notices can be found within the GDPR. Where possible retention periods should be included within your privacy notices, where this is not possible the criteria used to set retention periods should be included.

Subject access requests

Q: Does a subject access request require every document containing personal data to be sent or just details of the personal data held and in what form it was gathered, kept, secure etc?

A: Subject access requests relate to a copy of the personal data, not the document the personal data is contained within. The requirements for what such responses should contain are listed within the GDPR. Further information on this can be found on the ICO website under "Principle 6 – rights".

Data erasure, processing and breaches

Q: If a client asks us to stop processing, or erase their record. Would you expect brokers to pass that request to yourselves to ensure as much of the chain responds to the request?

A: If a controller receives a request for erasure they must notify anyone to whom it has disclosed the data unless it is impossible or would involve disproportionate effort.

Q: What defines a data processor?

A: The definition can be found within the GDPR, of which "Processor" means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller". This definition has not changed under the GDPR.

GDPR webinar – supporting you on your voyage to compliance
Q&As

Q: Should we see the Hiscox breach response policy? It may detail how you would tell brokers, if the brokers' policies data was breached inside the Hiscox network?

A: In the event of a data breach within Hiscox, as required we will contact relevant organisations and customers.

B2B and GDPR

Q: Do the updated consent requirements apply in business to business marketing or only "consumer" marketing? For example, can we still cross sell commercial insurance products to our existing commercial client base? Or do we need to update consent for this too?

A: The consent requirements apply wherever you are using consent as your legal basis of processing for personal data. You will need to review this alongside the PECR requirements to identify what action you need to take.

Q: Understand that the new regulations apply to natural persons – is it correct to assume they do not apply to commercial firms, partnerships, companies etc?

A: The GDPR applies to natural persons. Corporate entities data is not personal data unless a person can be specifically identified by it, e.g. directors' details.

Q: The obligations of a business when dealing B2C is quite clear, but what obligations does a company have under GDPR when dealing with B2B?

A: To the extent there is personal data the GDPR will apply.

Transport Layer Security (TLS)

Q: What is TLS?

A: Transport Layer Security (TLS) is an encryption protocol used to protect data in transit between computers. When two computers send data they agree to encrypt the information in a way they both understand. Depending on the rules in place, one or other of them may refuse to connect if they can’t find a suitable encryption method.

Q: What will Hiscox do if TLS isn't supported by the recipient?

A: In an email exchange the sending server contacts the receiving server over a standard SMTP connection and asks if it will accept a more secure TLS connection. As it does this, it shares a list of protocols and ciphers it understands. The receiving server looks at the list and chooses an option they both understand. It then sends back its security certificate and public encryption key.

The sending server checks the security certificate is valid, then uses the public key to encrypt and send an email. Only the receiving server has the private key that can decrypt the email, so the message is sent securely.

If either server can’t support an encrypted connection then they will default to a less secure connection such as Secure Sockets Layer (SSL) or a non-encrypted connection.

Q: Is TLS industry wide or will we have different systems with different insurers

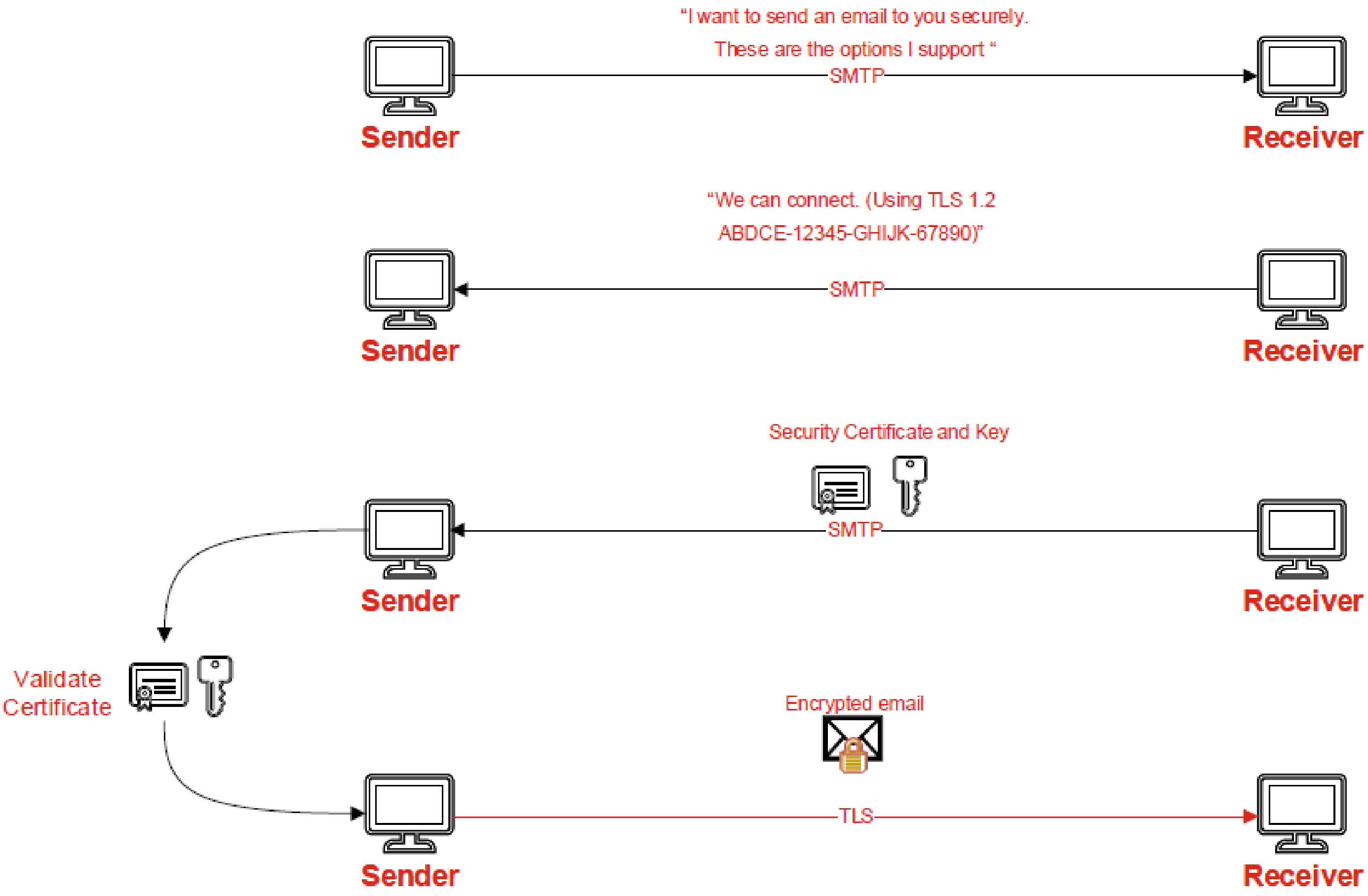
A: All modern email services should be capable of using TLS. In most cases there is the option of enabling opportunistic TLS on all connections. This means the servers will try to create an encrypted connection, but if they can’t they’ll send/receive unencrypted. Whilst opportunistic encryption will often be successful in sending encrypted emails it is not guaranteed.

To ensure that emails are always sent securely between two domains a rule needs to be created to enforce a TLS connection. When enforced any connections not using TLS will be automatically rejected, therefore this should ideally be enabled by both parties so that encryption is guaranteed and communications are not impeded.

GDPR webinar – supporting you on your voyage to compliance
Q&As

Q: What will Hiscox do if TLS isn't enforced by the recipient?

A: Some third parties already have enforced TLS links with Hiscox. Where this is not enabled we have opportunistic TLS. This means it will attempt to send the email via TLS and having analysed our outgoing emails this has a high success rate. However it is not guaranteed unless this link is enforced. We will continue with opportunistic TLS, whilst more enforced links are enabled. This diagram below may help explain how this works:


"I want to send an email to you securely.
These are the options I support "
SMTP
Sender
Receiver
"We can connect. (Using TLS 1.2
ABDCE-12345-GHIJK-67890)"
SMTP
Sender
Receiver
Security Certificate and Key
SMTP
Sender
Receiver
Validate Certificate
Encrypted email
TLS
Sender
Receiver

GDPR compliance may feel like a daunting journey ahead, Hiscox would like to support you where we can, should you have any further questions not covered above please feel free to email the GDPR team at UK&IGDPR@hiscox.com.