Using Personal Devices for Business: What Should UK Firms Think About?

14 April 2023

Following recent enforcement action by the UK Prudential Regulation Authority (the "PRA") against Wyelands Bank, which was partly based on its failure to retain business-related messages exchanged by senior executives and directors, regulated firms may want to review how they handle employees' use of personal devices for work purposes. The PRA strongly criticised Wyelands' lack of record-keeping policies and procedures to manage the use of WhatsApp communications, which the PRA found had prevented the bank's Board and Risk function from effectively scrutinising transactions, as well as hindering the PRA's supervision and investigation activities.[1]

The importance of this issue is reinforced by reports late last year that the Supervision division of the UK Financial Conduct Authority (the "FCA") had sent information requests to a number of firms regarding the use of private 'off-channel' messaging apps. In January 2021, the FCA had already highlighted the challenges and risk of misconduct arising from the increasing use of unmonitored or encrypted communication tools, emphasising that communications must be recorded and auditable.[2] U.S. authorities also imposed penalties totalling almost $2 billion against firms last year on the same topic.[3]

What are the UK Requirements? UK rules applying to regulated entities do not prevent the use of personal devices or messaging apps to conduct business. However, in brief, firms are obliged to:

- Take all reasonable steps to prevent employees from sending or receiving electronic communications on privately-owned equipment that the firm cannot copy;

---

1 PRA Final Notice – Wyelands Bank plc, 4 April 2023 https://www.bankofengland.co.uk/news/2023/april/pra-censures-wyelands-bank-plc-for-breaching-large-exposure-limits-and-failings.

2 FCA Market Watch 66, 11 January 2021 https://www.fca.org.uk/publications/newsletters/market-watch-66.

3 For a U.S. perspective, see our recent publications: https://www.debevoise.com/insights/publications/2023/03/doj-issues-trio-of-updates-that-further-heighten and https://www.debevoise.com/insights/publications/2023/02/reuters-the-messaging-dilemma.

- Retain a copy of electronic communications relating to a specified, but very broad, range of business activities for five years (or up to seven years where requested by the FCA); and

- Implement systems and controls to ensure compliance with the monitoring and record-keeping requirements outlined above (the same rules also apply to telephone conversations).

What Action Should Firms Take? Different approaches may be required depending on existing practices and the communication tools being used. It is possible for off-channel communications to continue, but there needs to be some way either to record these automatically (with monitoring software) or else ensure that they are captured and filed soon afterwards (which may be a manual process). Firms should consider:

- Regularly reviewing and tailoring their policies and procedures, especially to adapt to new communication apps and changing work practices;

- Clearly communicating any changes (or reinforcing existing procedures) to all staff, including a note from senior management;

- Asking staff to provide a specific periodic attestation that they are adhering to the procedures;

- Monitoring and testing compliance with the procedures, e.g. by sample testing whether all key communications with the customer or counterparty relating to a particular investment or trade can be identified in the firm's systems and records;

- Reviewing the appropriateness of using tools that can be downloaded onto employees' mobile devices to retain business data; and

- Establishing the duration and scope of historical non-compliance, so that they know where there are likely to be gaps in record-keeping.

Similar considerations may also arise for firms when dealing with the use of novel communication platforms on business devices.

What Data Privacy Issues Could This Raise? In developing and implementing policies to address the use of personal devices for business purposes, firms in the UK will need to consider carefully additional complications posed by the UK General Data Protection Regulation ("GDPR"). GDPR obligations are not avoided merely because a policy is directed at business information on a personal device.

Establishing a lawful basis for monitoring and accessing employees' personal devices can be particularly challenging, especially where such access is broad in scope or undertaken on an ongoing basis. There are difficult questions regarding if and when consent will be a lawful basis for such processing, and if not, the circumstances in which firms may be able to rely on other grounds (such as being necessary for compliance with legal obligations, or legitimate interest). In all cases, firms will want to ensure they are communicating with employees in a direct and transparent manner about how their personal data is handled and to process such data with great care, given the risk of incidentally or inadvertently collecting non-business-related personal data.

Karolos Seeger
Partner, London
+44 20 7786 9042
kseeger@debevoise.com

Robert Maddox
International Counsel, London
+44 20 7786 5407
rmaddox@debevoise.com

Aisling Cowell
Associate, London
+44 20 7786 9032
acowell@debevoise.com

Andrew Lee
Associate, London
+44 20 7786 9183
ahwlee@debevoise.com

Tristan Lockwood
Associate, London
+44 20 7786 3046
tlockwood@debevoise.com