Definitions

The exemptions apply to personal data used for "research purposes". Section 33 of the DPA states that "research purposes include statistical or historical purposes"—none of these terms are further defined. In the *Concise Oxford English Dictionary* "research" is defined as: 18–22

> "the systematic investigation into and study of materials and sources in order to establish facts and reach new conclusions."

"Statistical purposes" are presumably aimed at the study of or the production of statistics. "Historical purposes" could reasonably be regarded as covering historical studies. However, these are only specific elements covered by the definition and "research purposes" may be substantially wider than these two. As the exemption does not depend solely on just fulfilling the definition of "research" but is also dependent on satisfying the safeguard conditions it does not appear to be particularly material that the definition of "research" is a broad one. Therefore, "research" may be pure academic or "blue sky" research, targeted commercial research, or anything in between, including market research into consumers' attitudes. In the area of medical research the term will cover epidemiological studies and clinical studies. However, research will only qualify for one or more of the exemptions if it fulfils the safeguard conditions. These vary with the particular exemption involved.

EFFECT OF THE DPA ON RESEARCH

Three provisions of the DPA appear to have most impact on the use of personal data for research. 18–23

Grounds for legitimate processing

The use of personal data for research is not of itself a legitimating ground for processing. The two grounds which might be expected to be relied upon by researchers are: Ground 1, that the data subject has consented to the processing; and Ground 6, that the processing is "necessary" for the purposes of legitimate interests pursued by the data controller or by the third party or third parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject. In the case of research required by law, for example for pharmaco-vigilance referred to above, Ground 3 may be relevant provided that the personal data collected are deemed to adhere to the data minimisation principle. 18–24

The DSP opines on the correct interpretation if the word "necessary":

> "Data sharing may be 'necessary' ... if it is a proportionate method of achieving a legitimate objective: it need not be absolutely essentially to the achievement of that

> objective. Whether it is 'necessary' will depend on the circumstances of each case, including the sensitivity of the data and the effects that the disclosure may have on the data subjects and third parties."[52]

Whether or not this somewhat generous view of the extent of "necessity" (*R. V Secretary of State for Health, Ex p. C*[53]) would be upheld at the European level remains open to doubt as the DSP appears to truncate the test for assessing the legitimacy of an infringement of an art.8 right:

> "... 'necessary' in this context does not mean 'absolutely essential', and data sharing may meet this condition if it is a reasonable and proportionate way for a public body to give effect to its functions".[54]

The European jurisprudence in this area is more restrictive in its approach to any encroachment on an individual's art.8 right, with the test of "necessity" only arising if the domestic legislation authorising the disclosure of personal data:

> "... contain[s] detailed provisions circumscribing the scope of that power and providing safeguards against its arbitrary use".[55]

The House of Lords and House of Commons Joint Committee on Human Rights, Fourteenth Report, March 4, 2008, continues:

> "The right to respect for private life in Art.8 imposes a positive obligation on the State to ensure that the laws provide adequate protection against the unjustified disclosure of personal data."

If the domestic law does not meet the stringent requirements to ensure against the arbitrary use of personal data, then it cannot be "valid law" as it violates the European Convention on Human Right's requirements ab initio. Whether or not a United Kingdom legislative instrument meets European requirements is not a matter which the United Kingdom may decide solely for itself. In his 2008 article published in the May edition of "data protection law and policy", Douwe Korff, Professor of International Law, London Metropolitan University argues that the ECHR case of *Copland v United Kingdom (App. No.62617/00)*[56] illustrates this. In this case, the government argued that a public authority employer's monitoring of an employee's emails, telephone and internet usage was lawful because it was based on broad powers which authorised the public authority to do "anything necessary or expedient" for the purposes of providing higher education. The ECHR did not agree and held that at the relevant time there had been no valid law in the United Kingdom capable of being relied upon to justify the interference with the employee's art.8 rights. Professor Korff continues his analysis:

---

[52] *http://www.justice.gov.uk/information-access-rights/data-protection/data-sharing* [Accessed September 28, 2012], para.10.

[53] [2000] EWCA Civ 49, paras 16–20.

[54] *http://www.justice.gov.uk/information-access-rights/data-protection/data-sharing* [Accessed September 28, 2012], para 19

[55] *http://www.publications.parliament.uk/pa/jt200708/jtselect/jtrights/jtrights.htm* [Accessed September 28, 2012], p.7, para.11.

[56] [2007] All E.R. (D) 32 (Apr).