DIE RECHTE ANDERER BEACHTEN

— Wenn auf Ihren Fotos andere Menschen zum Motiv gehören, haben diese ein **Recht am eigenen Bild**. Sie müssen sie vorher fragen, bevor Sie die Fotos öffentlich ins Internet stellen. Das gleiche gilt für Videos.

— Fragen Dienste danach, ob sie nach Freunden suchen sollen, die den Dienst ebenfalls nutzen, sollte man nicht gleich »Ja« sagen. Es kann sein, dass der Anbieter dann unzählige **private E-Mail-Adressen** speichert, ohne dass die Betroffenen davon wissen.

— Wenn Sie Musik, Filme oder andere fremde Inhalte in öffentliche Ordner hochladen, können Sie **Urheberrechte** verletzen. Achten Sie ebenfalls darauf, Links auf solche Dateien nicht öffentlich im Internet zu verbreiten.

— Wenn Sie Dateien nur in der Familie oder mit Freunden über Cloud-Speicherdienste teilen, ist das als **Privatkopie** erlaubt.

iRIGHTS CLOUD
Das Informationsportal

iRights Cloud ist das Informationsportal zu rechtlichen, technischen und kulturellen Fragen zu Cloud Computing. Es ist eine digitale Anlaufstelle für nützliche Tipps, Hinweise und Checklisten und gibt Antworten auf Fragen wie:

— Was gibt es bei Cloud-Anbietern grundsätzlich zu beachten?
— Wann greift das Urheberrecht und welche Probleme ergeben sich dabei?
— Was bedeuten die Nutzungsbedingungen solcher Dienste?
— Welche Rolle spielt der Datenschutz?

Wir sind ein unabhängiges journalistisches Angebot, gefördert vom:

Bundesministerium für Ernährung, Landwirtschaft und Verbraucherschutz

www.cloud.irights.info

Ansprechpartner:
iRIGHTS CLOUD
Philipp Otto | Projektleiter | Almstadtstraße 9/11
D-10119 Berlin | otto@irights.info

SPEICHERN IN DER CLOUD

Die neuen Dienste richtig nutzen.

www.cloud.irights.info

DAS SIND CLOUD-SPEICHERDIENSTE

— Cloud-Speicherdienste erlauben es, Dateien nicht nur auf einzelnen Geräten zu speichern, sondern im Internet. Dadurch kann man von überall auf seine Dateien zugreifen – mit dem Rechner, dem Tablet oder dem Handy.

— Manche Anbieter nennen es »Cloud«, bei anderen heißt es »Online-Festplatte«. Das Prinzip ist dasselbe. Man kann seine Dateien über mehrere Geräte hinweg nutzen und bearbeiten oder mit anderen Nutzern teilen.

DIE WAHL DES ANBIETERS

— Für Cloud-Speicherdienste aus Europa sind die Anforderungen an den **Datenschutz** vom Gesetz her höher als in den USA.

— Das heißt aber nicht, dass **europäische Anbieter** automatisch sicherer sind. Einige Dienste haben sich bisher nicht dazu geäußert, wo die Daten konkret gespeichert werden.

— Wie ein Anbieter die Daten der Nutzer verwenden darf, wird vor allem in den **Nutzungsbedingungen** (Allgemeine Geschäftsbedingungen) und Datenschutzerklärungen geregelt. Informieren Sie sich über die Anbieter und stimmen Sie solchen Bedingungen nicht einfach zu.

BEI DIENSTEN ANMELDEN – MIT BEDACHT

— Sie dürfen für Benutzerkonten **Pseudonyme** und Phantasie-Angaben benutzen, wenn echte Daten nicht unbedingt erforderlich sind – zum Beispiel für die Abrechnung von Gebühren.

— Verwenden Sie unterschiedliche **Passwörter** für verschiedene Dienste. Ändern Sie Passwörter regelmäßig. Namen, Geburtstage und ähnliches sind keine guten Passwörter.

— Bei den meisten Anbietern können Sie aussuchen, ob Sie Dateien nur für sich, für ausgewählte Nutzer oder für alle öffentlich im Internet speichern. Schauen Sie sich die verschiedenen **Voreinstellungen** Ihres Dienstes genau an.

— **Überprüfen** Sie diese Einstellungen regelmäßig und ändern Sie diese nach Ihren Vorstellungen.

PRIVATE DATEN SCHÜTZEN

— Entscheiden Sie bewusst, **welche Daten** Sie Cloud-Speicherdiensten anvertrauen wollen.

— Nutzen Sie besonders auf **mobilen Geräten** zusätzliche Sicherheitseinstellungen wie PIN- oder Kennwort-Abfragen für Cloudspeicher-Apps.

— Vertrauen Sie nicht allein der Verschlüsselungstechnik der Anbieter. **Verschlüsseln Sie** nach eigenem Ermessen Ihre Daten, besonders bei sensiblen privaten Dokumenten.

— Zusätzliche **Verschlüsselungsprogramme** sind kostenlos erhältlich und heutzutage nicht mehr schwierig zu bedienen. Im Alltag funktionieren sie ähnlich wie ein Laufwerk oder Ordner auf Ihrem Rechner. Beispiele sind die Programme Boxcryptor, Truecrypt oder Cloudfogger.

— Vor den **Überwachungsprogrammen** der Geheimdienste im Internet, die in letzter Zeit bekannt geworden sind, gibt es nach derzeitigen Erkenntnissen keine umfassende Sicherheit.

— Wer technisch versiert ist, kann sich mit einem Computer, entsprechenden Programmen und einer Internetverbindung auch einen **eigenen Online-Speicher** bauen. Anleitungen dafür findet man im Internet.